Dell™ AppAssure™ 5.4.3

Guia de instalação e atualização

Se você tem quaisquer dúvidas ou perguntas sobre seu potencial uso deste material, entre em contato com:

Dell Inc.
Attn: LEGAL Dept
5 Polaris Way
Aliso Viejo, CA 92656

Consulte o nosso website (software.dell.com) para obter informações de contato de escritórios regionais e internacionais.

Marcas registradas

Legendas

△ CUIDADO: **o ícone de CUIDADO indica a possibilidade de danos ao hardware ou perda de dados caso as instruções não sejam seguidas.**

⚠ AVISO: **o ícone de AVISO indica a possibilidade de danos à propriedade, ferimentos pessoais ou morte.**

ⓘ **NOTA IMPORTANTE**, **NOTA**, **DICA**, **MÓVEL** ou **VÍDEO:** o ícone de informações indica uma informação extra/de apoio.

Dell AppAssure
Guia de instalação e atualização
Atualizado - Dezembro de 2014
Versão de software - 5.4.3

Conteúdo

1

Introdução ao AppAssure

Este capítulo fornece uma introdução e uma visão geral do AppAssure. Ele descreve os recursos, a funcionalidade e a arquitetura, e consiste nos seguintes tópicos:

- Principais tecnologias do AppAssure
- Arquitetura True Scale do AppAssure
- Arquitetura de implementação do AppAssure
- Recursos do produto do AppAssure

O AppAssure estabelece um novo padrão de proteção de dados unificada, combinando backup, replicação e recuperação em uma única solução, projetada para ser o backup mais rápido e confiável para a proteção de máquinas virtuais (VM), ambientes físicos e de nuvem.

O AppAssure combina backup e replicação em um produto de proteção de dados integrada e unificada, que também fornece reconhecimento do aplicativo para garantir uma recuperação confiável de dados de aplicativo a partir dos backups. O AppAssure se baseia na nova arquitetura True Scale™ (patente pendente), que proporciona o desempenho de cópia de segurança mais rápido com objetivos de tempo de recuperação (RTO) e objetivos de ponto de recuperação (RPO) muito agressivos, próximos de zero.

O AppAssure combina várias tecnologias exclusivas, inovadoras e avançadas:

- Live Recovery
- Verified Recovery
- Universal Recovery
- True Global Deduplication

Essas tecnologias são projetadas com integração segura para a recuperação após desastres na nuvem e proporcionam uma recuperação rápida e confiável. Com seu armazenamento escalável de objetos, o AppAssure tem uma capacidade exclusiva de processar petabytes de dados muito rapidamente, com eliminação da duplicação de dados global embutida, compactação, criptografia e replicação para qualquer infraestrutura de nuvem pública ou privada. Aplicativos e dados de servidor podem ser recuperados em minutos, para fins de retenção de dados e conformidade.

As ferramentas de cópia de segurança legadas atuais e as ferramentas de cópia de segurança com VM da primeira geração são ineficientes e ineficazes. As ferramentas de cópia de segurança desatualizadas não têm capacidade de trabalhar com dados em grande escala e não oferecem o nível de desempenho e confiabilidade necessário para proteger aplicativos críticos para os negócios. A combinação dessas características com ambientes de TI complexos e mistos representa um desafio administrativo para os profissionais de TI e vulnerabilidades para os dados do sistema.

O AppAssure enfrenta essa complexidade e ineficiência com a nossa tecnologia de core e suporte de ambientes com vários hypervisors, incluindo os que executam em VMware vSphere e Microsoft Hyper-V, que englobam nuvens públicas e privadas. O AppAssure oferece esses avanços tecnológicos e, ao mesmo tempo, reduz drasticamente os custos de gerenciamento de TI e armazenamento.

Principais tecnologias do AppAssure

Detalhes sobre as principais tecnologias do AppAssure são descritos nos tópicos a seguir.

Live Recovery

Live Recovery é uma tecnologia de recuperação instantânea para VMs ou servidores. Oferece acesso quase contínuo a volumes de dados em servidores virtuais ou físicos. É possível recuperar um volume inteiro com RTO próximo de zero e RPO de minutos.

A tecnologia de cópia de segurança e replicação do AppAssure registra snapshots simultâneos de várias VMs ou servidores, proporcionando proteção quase instantânea de dados e do sistema. É possível retomar o uso do servidor diretamente do arquivo de cópia de segurança, sem esperar uma restauração completa para o armazenamento de produção. Os usuários mantêm a produtividade e os departamentos de TI reduzem as janelas de recuperação para cumprir os contratos de nível de serviço atuais de RTO e RPO, cada vez mais exigentes.

Verified Recovery

O Verified Recovery permite realizar testes de recuperação e confirmação de cópias de segurança de forma automatizada. Ele inclui, entre outros, os sistemas de arquivo: Microsoft Exchange Server 2007, 2010 e 2013; e Microsoft SQL Server 2005, 2008, 2008 R2, 2012 e 2014. O Verified Recovery fornece capacidade de recuperação de aplicativos e cópias de segurança em ambientes físicos e virtuais. Ele também oferece um algoritmo abrangente de verificação de integridade, baseado em chaves de SHA de 256 bits que verificam a correção de cada bloco do disco na cópia de segurança durante as operações de arquivamento, replicação e propagação de dados. Essa capacidade garante a identificação precoce da corrupção de dados e impede que os blocos de dados corrompidos sejam mantidos ou transferidos durante o processo de cópia de segurança.

Universal Recovery

A tecnologia Universal Recovery oferece uma flexibilidade ilimitada de restauração de máquina. É possível restaurar suas cópias de segurança de um meio físico para virtual, de virtual para virtual, de virtual para físico ou de físico para físico. Também é possível realizar bare metal restores para hardware distinto; por exemplo, P2V, V2V, V2P, P2P, P2C, V2C, C2P e C2V.

Também acelera as movimentações entre plataformas entre as máquinas virtuais, por exemplo: mover de VMware para Hyper-V ou de Hyper-V para VMware. Baseia-se na recuperação no nível de aplicativo, nível do item e nível do objeto: arquivos individuais, pastas, e-mail, itens de calendário, bancos de dados e aplicativos. Com o AppAssure, também é possível recuperar ou exportar de físico para a nuvem ou do virtual para a nuvem.

True Global Deduplication

O AppAssure fornece a true global deduplication, que reduz drasticamente os requisitos de capacidade do disco físico, oferecendo taxas de redução de espaço que passam de 50:1 e, mesmo assim, atendem aos requisitos de armazenamento de dados. A compressão embutida no nível do bloco da arquitetura True Scale e a deduplicação com desempenho com velocidade de linha, juntamente com a verificação de integridade embutida, impede que a corrupção dos dados afete a qualidade dos processos de cópia de segurança e arquivamento.

Arquitetura True Scale do AppAssure

O AppAssure foi desenvolvido com a arquitetura True Scale do AppAssure. Utiliza uma arquitetura dinâmica, de pipeline e de vários cores otimizada para proporcionar consistentemente um desempenho com velocidade de linha para ambientes corporativos. A arquitetura True Scale é projetada de forma ascendente para escalar linearmente e armazenar e gerenciar big data eficientemente e fornecer RTOs e RPOs de minutos sem

comprometer o desempenho. Inclui um gerenciador de objeto e volume feito sob medida com deduplicação global, compressão, criptografia, replicação e retenção integradas. O diagrama a seguir descreve a arquitetura True Scale do AppAssure.

Figura 1. Arquitetura True Scale do AppAssure

O AppAssure Volume Manager e o armazenamento escalável de objetos atuam como a base da arquitetura True Scale do AppAssure. O armazenamento escalável de objetos armazena snapshots no nível do bloco que são capturados a partir de servidores virtuais e físicos. O gerenciador de volume gerencia os vários armazenamentos de objetos, fornecendo um repositório comum ou armazenamento just-in-time somente para o que é necessário. O armazenamento de objetos suporta tudo simultaneamente com I/O assíncrona, que proporciona alta taxa de transferência com latência mínima e maximiza a utilização do sistema. O repositório reside em tecnologias de armazenamento diferentes, como rede de área de armazenamento (SAN), armazenamento por conexão direta (DAS) ou armazenamento conectado à rede (NAS).

A função do AppAssure Volume Manager é similar à do gerenciador de volume em um sistema operacional. Ela seleciona vários dispositivos de armazenamento, que podem ser de diversos tipos e tamanhos, e os combina em volumes lógicos, usando políticas de alocação distribuídas ou sequenciais. O armazenamento de objetos salva, recupera, mantém e, em seguida, replica objetos derivados de snapshots que reconhecem os aplicativos. O gerenciador de volume proporciona um desempenho de I/O escalável em conjunto com deduplicação global de dados, criptografia e gerenciamento de retenção.

Arquitetura de implementação do AppAssure

O AppAssure é um produto escalável de backup e recuperação, implementado de forma flexível na empresa ou como um serviço prestado por um provedor de serviços gerenciados. O tipo de implementação depende do tamanho e dos requisitos do cliente. A preparação para implementar o AppAssure envolve o planejamento da topologia de armazenamento na rede, hardware do core e infraestrutura de recuperação após desastres e segurança.

A arquitetura de implementação do AppAssure consiste em componentes locais e remotos. Os componentes remotos podem ser opcionais para as pessoas que não querem usar um site de recuperação após desastres ou um provedor de serviços gerenciados para a recuperação fora do local. Uma implementação local básica consiste em um servidor de cópia de segurança chamado de Core e uma ou mais máquinas protegidas, conhecida como Agent. O componente fora do local é ativado usando a replicação que fornece recursos completos de recuperação no site de DR. O AppAssure Core usa imagens de base e snapshots incrementais para compilar pontos de recuperação de agentes protegidos.

Além disso, o AppAssure reconhece o aplicativo, pois tem a capacidade de detectar a presença do Microsoft Exchange, do SQL e seus respectivos bancos de dados e arquivos de log e, em seguida, agrupa esses volumes automaticamente com dependência, para uma proteção abrangente e uma recuperação efetiva. Isso impede que haja cópias de segurança incompletas quando você realizar recuperações. As cópias de segurança são realizadas usando snapshots no nível do bloco que reconhecem o aplicativo. O AppAssure também pode realizar o truncamento de log dos servidores protegidos do Microsoft Exchange e do SQL.

O diagrama a seguir descreve uma implementação simples do AppAssure. Nesse diagrama, os AppAssure Agents são instalados em máquinas, como um servidor de arquivos, de e-mail ou de banco de dados, ou em máquinas virtuais, conectam-se a um único AppAssure Core, que também é constituído pelo repositório central, e são protegidos por ele. O Portal de licenças do Dell AppAssure gerencia as assinaturas de licença, grupos e usuários para os agentes e cores do ambiente. Os usuários efetuam login no Portal de licenças para ativar contas, baixar o software e implementar agentes e cores de acordo com a licença para o seu ambiente.

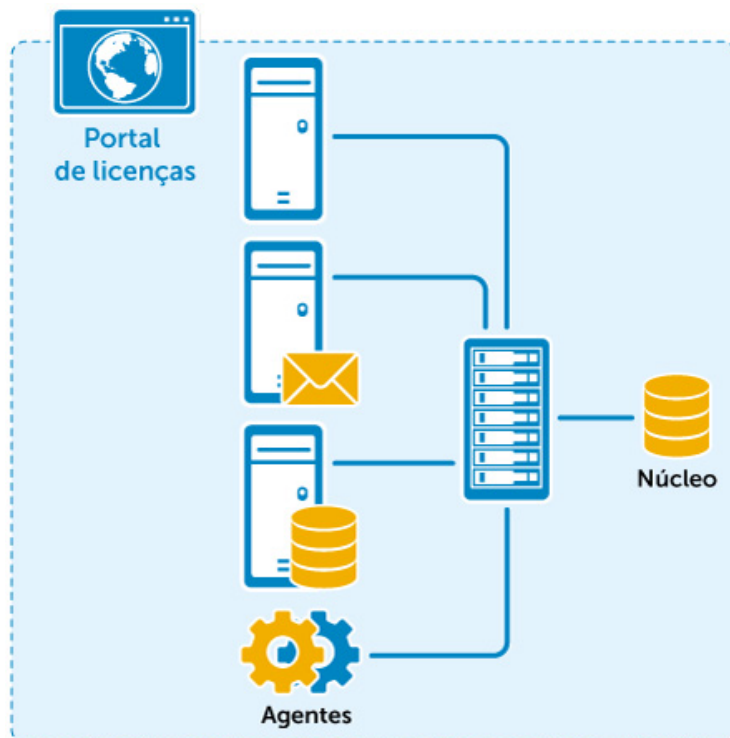
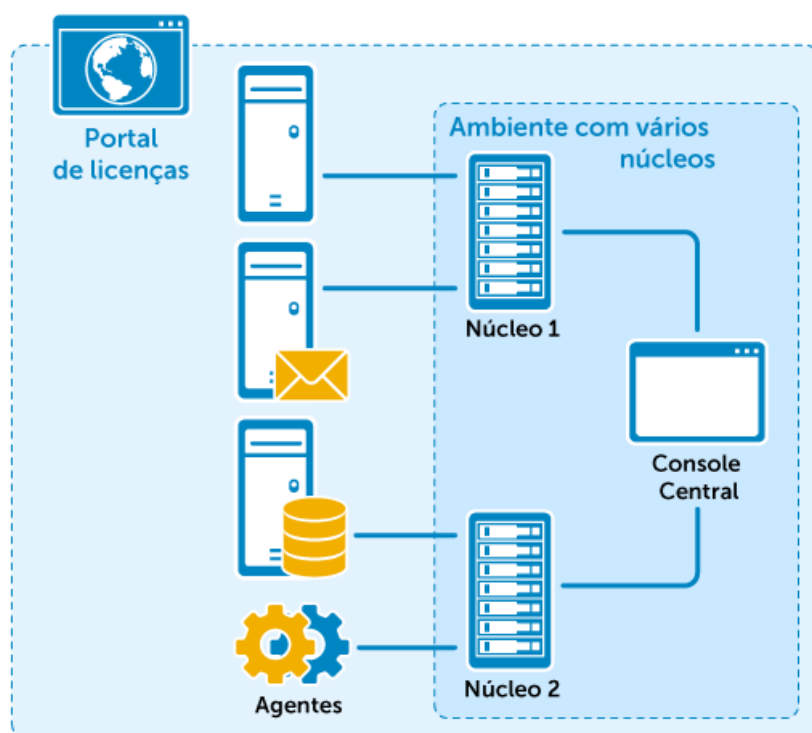
Figura 2. Arquitetura de implementação do AppAssure

Também é possível implementar vários AppAssure Cores, conforme exibido no diagrama a seguir. Um console central baseado na Web gerencia vários cores.

Figura 3. Arquitetura de implementação de vários Cores do AppAssure

AppAssure Smart Agent

O AppAssure Smart Agent é instalado nas máquinas que serão protegidas pelo AppAssure Core. O Smart Agent rastreia os blocos alterados no volume de disco e, em seguida, cria um snapshot de uma imagem dos blocos alterados em um intervalo de proteção predefinido. A abordagem "para sempre" desses snapshots incrementais no nível do bloco impede a repetição da cópia dos mesmos dados da máquina protegida para o Core. O Smart Agent reconhece o aplicativo e fica inativo quando não está em uso, com quase zero por cento (0%) de utilização da CPU e menos de 20 MB de sobrecarga de memória. Quando o Smart Agent está ativo, ele chega a dois (2%) a quatro por cento (4%) de utilização da CPU e menos de 150 MB de memória, que inclui a transferência dos snapshots para o Core. Esse valor é muito inferior ao dos programas de software legados tradicionais, que usam níveis muito mais altos de CPU e largura de banda da memória, mesmo estando inativos.

O AppAssure Smart Agent reconhece os aplicativos porque detecta não somente o tipo de aplicativo instalado, mas também a localização dos dados. Ele agrupa automaticamente os volumes de dados com dependência como os bancos de dados e, em seguida, registra-os juntos para uma proteção efetiva e recuperação rápida. Após a configuração do agente, ele usa a tecnologia inteligente para acompanhar os blocos alterados nos volumes de disco protegidos. Quando o snapshot está pronto, ele é transferido rapidamente para o AppAssure Core usando conexões inteligentes, de multiprocessamento e baseadas em soquetes. Para preservar a largura de banda da CPU e a memória nas máquinas protegidas, o Smart Agent não criptografa nem faz a deduplicação dos dados na origem, e as máquinas do agente são pareadas com um core para proteção.

AppAssure Core

O AppAssure Core é o componente central da AppAssure arquitetura de implementação. O Core armazena e gerencia todas as cópias de segurança da máquina e presta serviços essenciais de cópia de segurança, de recuperação e retenção, bem como de replicação, arquivamento e gerenciamento. O Core é um servidor dedicado independente endereçável na rede que executa uma variante de 64 bits do sistema operacional

Microsoft Windows. O AppAssure realiza compactação embutida, criptografia e deduplicação de dados baseada no destino dos dados recebidos a partir de um agente.

Em seguida, o Core armazena as cópias de segurança de snapshot em um repositório, que pode residir em diversas tecnologias de armazenamento, como rede de área de armazenamento (SAN), armazenamento com conexão direta (DAS) ou armazenamento conectado à rede (NAS). O repositório também pode residir em volumes de armazenamento interno no servidor Core. O Core é gerenciado acessando a seguinte URL em um navegador da Web habilitado para JavaScript: https://CORENAME:8006/apprecovery/admin. Internamente, todos os serviços do core podem ser acessados por meio das APIs (Application Programming Interfaces) REST (Representational State Transfer). Os principais serviços podem ser acessados de dentro do Core ou diretamente pela Internet, a partir de qualquer aplicativo que possa enviar uma solicitação de HTTP/HTTPS e receber uma resposta de HTTP/HTTPS. Todas as operações de API são realizadas em SSL e autenticadas mutuamente por meio de certificados X.509 v3.

Processo de snapshots

O processo de proteção do AppAssure começa quando uma imagem de base é transferida de uma máquina agente para o Core, seguida de snapshots incrementais para sempre. O software AppAssure Agent para Windows usa o Microsoft Volume Shadow Copy Service (VSS) para congelar e desativar os dados de aplicativo no disco a fim de capturar uma cópia de segurança consistente com o sistema de arquivos e com os aplicativos. Quando se cria um snapshot, o gravador do VSS no servidor de destino impede a gravação de conteúdo no disco. Durante o processo de impedir a gravação de conteúdo no disco, todas as operações de I/O no disco entram na fila e são retomadas somente depois que o snapshot é concluído; as operações ainda em andamento, por sua vez, serão concluídas e todos os arquivos abertos serão fechados. O processo de criar uma cópia de sombra não afeta muito o desempenho do sistema de produção.

O AppAssure usa o VSS da Microsoft porque ele tem suporte incorporado para todas as tecnologias internas do Windows, como NTFS, Registro, Active Directory, etc., para liberar dados para o disco antes do snapshot. Além disso, outros aplicativos corporativos, como o Microsoft Exchange e o SQL Server, usam plug-ins do VSS Writer para receber notificações quando um snapshot está sendo preparado e quando é necessário liberar as páginas de banco de dados usadas para o disco para que o banco de dados fique em um estado transacional consistente. É importante ressaltar que o VSS é usado para desativar os dados de sistema e aplicativo no disco; não é usado para criar o snapshot. Os dados capturados são transferidos rapidamente para o AppAssure Core e armazenados nele. O uso do VSS para a cópia de segurança não deixa o servidor de aplicativos no modo de cópia de segurança por um período longo, já que o tempo necessário para realizar o snapshot é medido em segundos e não em horas. Outro benefício do uso do VSS para cópias de segurança é o fato de ele permitir que uma máquina protegida obtenha um snapshot de grandes quantidades de dados simultaneamente, já que o snapshot funciona no nível do volume.

Replicação – Site de recuperação após desastres ou provedor de serviços

O processo de replicação no AppAssure requer um relacionamento pareado de origem/destino entre dois ou mais cores. Esse core de origem copia os pontos de recuperação de máquinas protegidas selecionadas e então transmite de modo assíncrono e contínuo os dados de snapshot incrementais para o core de destino em um site de recuperação após desastres remoto. O lugar externo pode ser um data center de propriedade da empresa (core autogerenciado), um local de terceiros de um provedor de serviços gerenciados (MSP) ou um ambiente de nuvem. Ao replicar para um core de destino de terceiros, é possível usar fluxos de trabalho incorporados que permitam solicitar conexões e receber notificações automáticas de feedback. Para a transferência inicial de dados, é possível realizar a propagação de dados usando mídias externas; isso é útil para grandes conjuntos de dados ou sites com links lentos.

No caso de uma interrupção grave, o AppAssure suporta a ativação e a reativação pós-falha em ambientes replicados. Em caso de interrupção ampla, o core de destino no site secundário pode recuperar instâncias de máquinas replicadas e iniciar imediatamente a proteção nas máquinas de ativação pós-falha. Depois que o site primário é restaurado, o core replicado pode realizar a reativação pós-falha dos dados a partir das instâncias recuperadas, devolvendo-os às máquinas protegidas no site primário.

Recuperação

A recuperação pode ser realizada no site local ou no site remoto replicado. Quando a implementação está no estado estável com proteção local e replicação opcional, o AppAssure Core permite realizar a recuperação usando Verified Recovery, Universal Recovery ou Live Recovery.

Recursos do produto do AppAssure

Usando o AppAssure, você pode gerenciar todos os aspectos de proteção e recuperação de dados críticos por meio dos seguintes recursos e funcionalidades. Eles incluem:

- Repositório
- True Global Deduplication
- Criptografia
- Replicação
- Recovery-as-a-Service (RaaS)
- Retenção e arquivamento
- Virtualização e nuvem
- Gerenciamento de eventos e alertas
- Portal de licenças
- Console da Web
- APIs de gerenciamento de serviço
- Atribuição de marca branca
- Assistentes AppAssure

Repositório

O repositório do AppAssure usa o gerenciador de volume para deduplicação (DVM) para implementar um gerenciador de volumes que oferece suporte a vários volumes, sendo que cada um deles pode residir em diversas tecnologias de armazenamento, como rede de área de armazenamento (SAN), armazenamento com conexão direta (DAS), armazenamento conectado à rede (NAS) ou armazenamento na nuvem. Cada volume consiste em um armazenamento escalável de objetos com deduplicação. O armazenamento escalável de objetos se comporta como um sistema de arquivos baseado em registros, em que a unidade de alocação de armazenamento é um bloco de dados com tamanho fixo, conhecido como registro. Esta arquitetura permite configurar o suporte do tamanho do bloco para compressão e deduplicação. As operações de rollup são reduzidas a operações de metadados a partir de operações com uso intenso do disco, porque o rollup não movimenta mais os dados, movimenta apenas os registros.

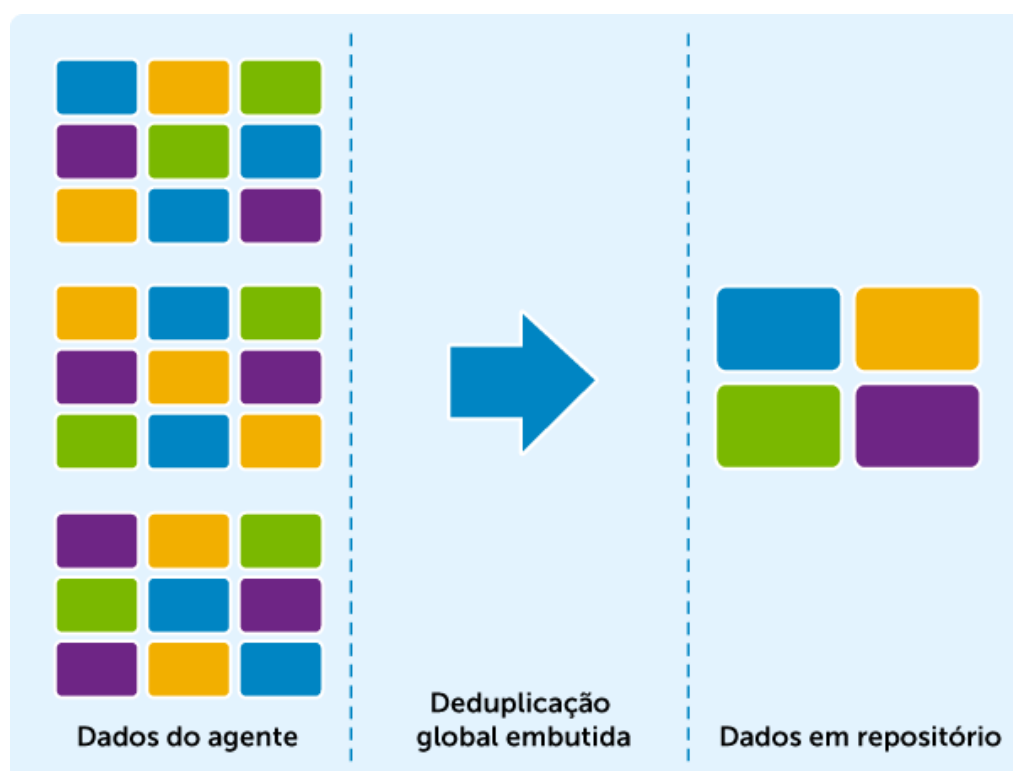
O DVM pode combinar um conjunto de armazenamentos de objetos em um volume, e eles podem ser expandidos pela criação de sistemas de arquivos adicionais. Os arquivos do armazenamento de objetos são pré-alocados e podem ser adicionados sob demanda conforme os requisitos de armazenamento se alteram. É possível criar até 255 repositórios independentes em um único AppAssure Core e aumentar mais o tamanho de um repositório adicionando novas extensões de arquivo. Um repositório estendido pode conter até 4.096 extensões que abrangem diversas tecnologias de armazenamento. O tamanho máximo dos repositórios é 32 Exabytes. Um único core pode ter vários repositórios.

True Global Deduplication

O True Global Deduplication é um método efetivo de redução das necessidades de armazenamento de cópia de segurança, eliminando dados redundantes ou duplicados. A deduplicação é efetiva porque somente uma instância dos dados em várias cópias de segurança é armazenada no repositório. Os dados redundantes são armazenados, mas não fisicamente; eles são simplesmente substituídos por um indicador que aponta para a instância única dos dados no repositório.

Os aplicativos convencionais de cópia de segurança realizam cópias de segurança completas repetitivas semanalmente, mas o AppAssure realiza cópias de segurança incrementais das máquinas no nível do bloco para sempre. Essa abordagem incremental para sempre, em conjunto com a deduplicação de dados, ajuda a reduzir drasticamente o total de dados gravados no disco.

O layout de disco típico de um servidor é constituído pelo sistema operacional, aplicativos e dados. Na maioria dos ambientes, os administradores frequentemente usam um tipo em comum de sistema operacional de desktop e server em vários sistemas, para que a implementação e o gerenciamento sejam efetivos. Quando o AppAssure faz uma cópia de segurança no nível do bloco em várias máquinas ao mesmo tempo, ele fornece uma visualização mais detalhada daquilo que está (e do que não está) na cópia de segurança, independentemente da origem. Esses dados incluem o sistema operacional, os aplicativos e os dados de aplicativo de todo o ambiente.

Figura 4. True Global Deduplication

O AppAssure realiza a deduplicação de dados embutida baseada no destino. Esse método transmite os dados de snapshot para o core antes de serem deduplicados. Deduplicação de dados embutida significa simplesmente que a duplicação dos dados é eliminada antes da confirmação no disco. Isso é muito diferente da deduplicação na origem ou após o processo, na qual a duplicação dos dados é eliminada na origem antes da transmissão; no pós-processo, os dados são enviados em forma bruta para o destino, onde são analisados e a duplicação é eliminada depois da confirmação dos dados no disco. A deduplicação de dados na origem consome recursos preciosos do sistema na máquina, ao passo que a abordagem de eliminação da deduplicação de dados pós-processo requer que todos os dados necessários estejam no disco (uma sobrecarga maior de capacidade inicial) antes de começar o processo de deduplicação. Por outro lado, a deduplicação de dados embutida não requer capacidade de disco adicional e ciclos de CPU na origem nem no Core para o processo de deduplicação. Para concluir, os aplicativos convencionais de cópia de segurança realizam cópias de segurança completas repetitivas toda

semana, enquanto que o AppAssure realiza cópias de segurança incrementais das máquinas no nível do bloco para sempre. Essa abordagem incremental para sempre, em conjunto com a deduplicação de dados, ajuda a reduzir drasticamente o total de dados gravados no disco, com uma proporção de redução de até 80:1.

Criptografia

O AppAssure fornece criptografia integrada para proteger cópias de segurança e dados em repouso contra o uso e acesso sem autorização, garantindo a privacidade dos dados. O AppAssure fornece criptografia forte. Ao fazer isso, as cópias de segurança de computadores protegidos ficam inacessíveis. Somente o usuário que tem a chave de criptografia pode acessar e descriptografar os dados. Não há limite para o número de chaves de criptografia que podem ser criadas e armazenadas em um sistema. O DVM usa a criptografia AES de 256 bits no modo encadeamento de blocos de codificação (CBC) com chaves de 256 bits. A criptografia é realizada de forma embutida nos dados de snapshot, a velocidades de linha, sem afetar o desempenho. Isso acontece porque a implementação do DVM é multiprocessamento e usa a aceleração de hardware específica para o processador no qual ele está implementado.

A criptografia está preparada para a multilocação. A deduplicação foi limitada especificamente aos registros que foram criptografados com a mesma chave; dois registros idênticos que foram criptografados com chaves diferentes não terão a deduplicação. Essa decisão de projeto impede que a deduplicação seja usada para vazar dados entre domínios de criptografia diferentes. Isso beneficia os provedores de serviços gerenciados, já que as cópias de segurança replicadas de vários locatários (clientes) podem ser armazenadas em um único core, sem que um locatário possa ver ou acessar os dados de outros locatários. Cada chave de criptografia de um locatário ativo cria um domínio de criptografia dentro do repositório, no qual somente o proprietário das chaves pode ver, acessar ou usar os dados. Em um cenário de multilocação, os dados são particionados e deduplicados dentro dos domínios de criptografia.

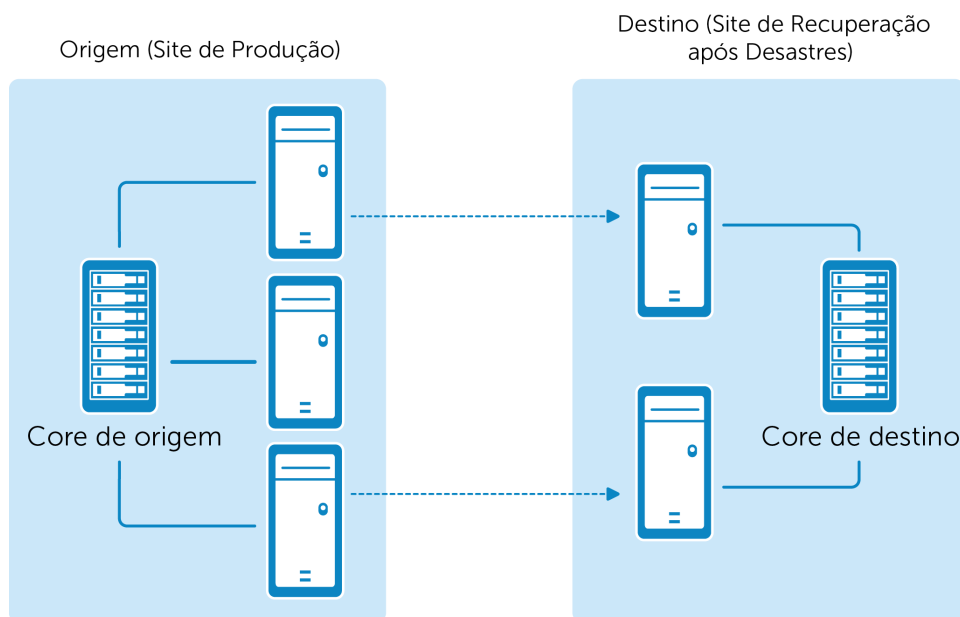
Nos cenários de replicação, o AppAssure usa o SSL 3.0 para proteger as conexões entre os dois cores em uma topologia de replicação para impedir espionagem e adulteração.

Replicação

Replicação é o processo de copiar pontos de recuperação de um core AppAssure e transmiti-los a outro core AppAssure em um local separado para fins de recuperação após desastres. O processo exige uma solução com pares de origem/destino entre dois ou mais cores.

Esse core de origem copia os pontos de recuperação de máquinas protegidas selecionadas e então transmite de modo assíncrono e contínuo os dados de snapshot incrementais para o core de destino em um site de recuperação após desastres remoto. É possível configurar a replicação de saída para um data center de propriedade da empresa ou para um site de recuperação após desastres remoto (ou seja, um core de destino "autogerenciado"). Ou é possível configurar a replicação de saída para um provedor de serviços gerenciados (MSP) terceirizado ou provedor de nuvem que hospede serviços de recuperação após desastres e cópia de segurança em um site externo. Ao replicar para um core de destino de terceiros, é possível usar fluxos de trabalho incorporados que permitam solicitar conexões e receber notificações automáticas de feedback.

A replicação é gerenciada por máquina protegida. Qualquer máquina (ou todas as máquinas) protegida ou replicada em um core de origem pode ser configurada para replicar em um core de destino.

Figura 5. Replicação

A replicação se otimiza com um algoritmo exclusivo de leitura-correspondência-gravação (RMW) acoplado fortemente à deduplicação. Na replicação RMW, o serviço de replicação de origem e destino faz a correspondência das chaves antes de transferir dados e, em seguida, replica somente os dados compactados, criptografados e de deduplicação pela WAN. Ao fazer isso, reduz em 10x os requisitos de largura de banda.

A replicação começa pela propagação, ou seja, a transferência inicial de imagens de base de deduplicação e snapshots incrementais dos agentes protegidos, que pode acrescentar centenas ou milhares de gigabytes de dados. A replicação inicial pode ser propagada para o core de destino usando mídias externas. Normalmente, isso é útil para grandes conjuntos de dados ou sites com links lentos. Os dados do arquivo de propagação são compactados e criptografados e a duplicação é eliminada. Se o tamanho total do arquivo for superior ao espaço disponível na mídia removível, o arquivo pode ocupar vários dispositivos, com base no espaço disponível nas mídias. Durante o processo de propagação, os pontos de recuperação incremental são replicados no site de destino. Depois que o core de destino consome o arquivo de propagação, os pontos de recuperação incremental recém-replicados são sincronizados automaticamente.

Recovery-as-a-Service (RaaS)

Os provedores de serviços gerenciados (MSPs) podem utilizar o AppAssure como uma plataforma para oferecer a recuperação como serviço (RaaS). A RaaS facilita a recuperação completa na nuvem replicando os servidores físicos e virtuais do cliente, juntamente com seus dados, para a nuvem do provedor de serviços como máquinas virtuais para suportar o teste de recuperação ou operações reais de recuperação. Os clientes que desejam realizar recuperação na nuvem podem configurar a replicação nas máquinas protegidas nos cores locais para um provedor de serviços do AppAssure. Em caso de desastre, os MSPs podem realizar instantaneamente o provisionamento das máquinas virtuais para o cliente.

Os MSPs podem implementar uma infraestrutura de RaaS com multilocação baseada em AppAssure que pode hospedar várias organizações ou unidades de negócios separadas (os locatários), que normalmente não compartilham segurança ou dados em um único servidor ou um grupo de servidores. Os dados de cada locatário são isolados e protegidos de outros locatários e do provedor de serviço.

Retenção e arquivamento

O AppAssure oferece políticas flexíveis de cópia de segurança e retenção fáceis de configurar. A capacidade de ajustar as políticas de retenção às necessidades de uma organização não só ajuda a preencher os requisitos de conformidade, mas também faz isso sem comprometer os objetivos de tempo de recuperação (RTO).

As políticas de retenção impõem períodos de tempo em que as cópias de segurança são armazenadas em mídias de curto prazo (rápidas e caras). Às vezes, certos requisitos técnicos e de negócios exigem a retenção prolongada dessas cópias de segurança, mas o armazenamento rápido tem um custo proibitivo. Portanto, esse requisito gera uma necessidade de armazenamento de longo prazo (lento e barato). As empresas frequentemente usam o armazenamento de longo prazo para arquivar dados de conformidade e não conformidade. O recurso de arquivamento suporta retenções prolongadas para dados de conformidade e não conformidade, além de ser usado para propagar dados de replicação para um core de destino.

Figura 6. Política de retenção

No AppAssure, as políticas de retenção podem ser personalizadas para especificar o tempo durante o qual um ponto de recuperação de cópia de segurança é mantido. Conforme o fim do período de retenção dos pontos de recuperação se aproxima, eles vencem e são removidos do grupo de retenção. Normalmente, esse processo se torna ineficiente e acaba falhando, já que a quantidade de dados e o período de retenção começam a aumentar rapidamente. O AppAssure resolve o problema do big data gerenciando a retenção de grandes quantidades de dados com políticas de retenção complexas e realizando operações de rollup para dados que estão vencendo, por meio de operações eficientes de metadados.

É possível realizar cópias de segurança com um intervalo de poucos minutos, e essas cópias de segurança vencem em dias, meses e anos. As políticas de retenção gerenciam o vencimento e a exclusão de cópias de segurança antigas. Um método simples em cascata define o processo de vencimento. Os níveis dentro da cascata são definidos em minutos, horas e dias; semanas, meses e anos. A política de retenção é imposta pelo processo noturno de rollup.

Para o arquivamento de longo prazo, o AppAssure permite criar um arquivo do core de origem ou destino em qualquer mídia removível. O arquivo é otimizado internamente, e todos os dados do arquivo são compactados, criptografados e têm deduplicação. Se o tamanho total do arquivo for superior ao espaço disponível na mídia removível, o arquivo ocupará vários dispositivos com base no espaço disponível nas mídias. A recuperação a partir de um arquivo não requer um novo core; qualquer core pode ingerir o arquivo e recuperar dados se o administrador tiver a frase de acesso e as chaves de criptografia.

Virtualização e nuvem

O AppAssure Core está preparado para a nuvem, permitindo que você utilize a capacidade computacional da nuvem para a recuperação e para o arquivamento.

O AppAssure pode exportar qualquer máquina protegida ou replicada para uma máquina virtual (VM), como a versão licenciada do VMware ou Hyper-V. É possível realizar uma exportação virtual de uma vez ou estabelecer uma máquina virtual em modo de standby virtual ao estabelecer uma exportação virtual contínua. Nas

exportações contínuas, a máquina virtual é atualizada de forma incremental depois de cada snapshot. As atualizações adicionais são rápidas e fornecem clones em estado de espera prontos para serem acionados com um clique em um botão. Tipos de exportação de VM suportados incluem: VMware Workstation e VMWare Server em uma pasta; exportação direta para um host do vSphere ou VMware ESX(i); exportação para o Oracle VirtualBox; e exportação para o Microsoft Hyper-V Server no Windows Server 2008 (x64), 2008 R2, 2012 (x64) e 2012 R2 (incluindo suporte para as máquinas virtuais Hyper-V geração 2).

Além disso, é possível arquivar seus dados do repositório na nuvem utilizando o Microsoft Azure, Amazon S3, Rackspace Cloud Files ou outros serviços de nuvem baseados em OpenStack.

Gerenciamento de eventos e alertas

Além das APIs de REST HTTP, o AppAssure também inclui um conjunto amplo de recursos para a criação de logs e a notificação de eventos usando e-mail, syslog ou o Log de eventos do Windows. As notificações por e-mail podem ser usadas para alertar os usuários ou grupos sobre o funcionamento ou o status de diversos eventos em resposta a um alerta. Os métodos do syslog e do Log de Eventos do Windows são usados para a criação de logs centralizada em um repositório, em ambientes com vários sistemas operacionais; por outro lado, em ambientes que só têm Windows, apenas o Log de Eventos do Windows é usado.

Portal de licenças

O Portal de licenças do Dell AppAssure fornece ferramentas fáceis de usar para gerenciar os direitos de licença. É possível baixar, ativar, ver e gerenciar chaves de licença e criar um perfil de empresa para rastrear os ativos de licença. Além disso, o portal permite que os provedores de serviços e revendedores rastreiem e gerenciem as licenças de cliente.

Console da Web

O AppAssure tem um console central baseado na Web que gerencia cores distribuídos do AppAssure a partir de um local central. Os provedores de serviços gerenciados (MSPs) e clientes corporativos com vários cores distribuídos podem implementar esse console para obter uma visualização unificada para um gerenciamento centralizado. O AppAssure Central Management Console permite organizar os cores gerenciados em unidades organizacionais hierárquicas. Essas unidades organizacionais podem representar unidades de negócios, locais ou clientes para os MSPs com acesso baseado em função. Usando o console central, você também pode executar relatórios em todos os cores gerenciados.

APIs de gerenciamento de serviço

O AppAssure vem com um conjunto de APIs de gerenciamento de serviços e fornece acesso programático a todas as funcionalidades disponíveis por meio do AppAssure Central Management Console. A API de gerenciamento de serviços é uma API de REST. Todas as operações de API são realizadas em SSL e autenticadas mutuamente por meio de certificados X.509 v3. O serviço de gerenciamento pode ser acessado de dentro do ambiente ou diretamente pela Internet, a partir de qualquer aplicativo que possa enviar e receber solicitações e respostas de HTTPS. A abordagem facilita a integração fácil a qualquer aplicativo da Web, como ferramentas de metodologia de gerenciamento de relacionamentos (RMM) ou sistemas de faturação. Um cliente de SDK para PowerShell scripting também está incluído no AppAssure.

Atribuição de marca branca

O AppAssure pode ter a marca alterada ou ser comercializado sem marca para parceiros corporativos e de OEM selecionados, de acordo com o programa de provedor de serviços Platinum. Com o programa de provedor de serviços Platinum, os parceiros podem usar seu nome, logotipo e cores no AppAssure e fornecer o produto ou serviço com sua própria marca e visual para os clientes.

Como parceiro do AppAssure, você pode ajustar o software para que ele atenda aos seus requisitos de negócios. Para saber mais sobre a forma de uso da sua marca no AppAssure visando a suprir as suas necessidades de negócios, entre em contato com o Departamento de Vendas Dell AppAssure pelo e-mail sales@software.dell.com para obter mais informações.

Assistentes AppAssure

O assistente é um conjunto de etapas guiadas apresentadas ao usuário em uma janela pop-up para automatizar uma tarefa complexa ou mais. Por definição, os assistentes contêm duas páginas de informações (ou mais) para o usuário preencher. (Um pop-up de janela única é considerado simplesmente como uma caixa de diálogo). Os assistentes usam diversas convenções gráficas bastante conhecidas para coletar informações, como caixas de texto, botões de opções, caixas de verificação e menus suspensos.

Quando um assistente é iniciado, uma janela se abre acima da interface do usuário e o orienta em uma série de opções necessárias para realizar a tarefa. Você segue as informações apresentadas em cada página do assistente, conforme os seus requisitos, navegando pelas páginas do assistente por meio dos botões **Avançar** e **Voltar**. Ao terminar, você clica em um botão de enviar (para confirmar suas opções e realizar a tarefa) ou no botão **Cancelar** (para cancelar sem fazer alterações e voltar à UI na qual você abriu o assistente).

O AppAssure oferece vários assistentes, que podem ser divididos em duas categorias.

Primeiramente, há assistentes para instalar, atualizar ou remover o software AppAssure e os componentes relacionados. Normalmente, eles são iniciados ao clicar duas vezes em um programa executável de instalador de software. Os instaladores podem ser acessados ao fazer o download de componentes específicos do Portal de licenças do Dell AppAssure.

Em segundo lugar, os assistentes estão disponíveis na interface de usuário do AppAssure Core Console. Normalmente, eles são lançados ao clicar em um botão ou link rotulado com a função ou o resultado do assistente. Os assistentes dessa categoria são listados a seguir.

Tabela 1.

Nome do assistente	Iniciado por	Descrição
Guia de início rápido	Opção Guia de início rápido (menu Ajuda)	Unifica vários fluxos de trabalho para simplificar tarefas comuns do AppAssure. Guia o usuário no processo de proteger máquinas, configurar a replicação em novos agentes, exportar dados protegidos para máquinas virtuais, criptografar dados dos pontos de recuperação, configurar grupos de notificação por e-mail e configurar uma política de retenção.
Assistente de proteção de máquina	Botão Proteger máquina (barra de botões)	Configura a proteção em uma máquina que você especifica. Permite dar um nome à máquina para ser exibido no console do Core. Se o software Agent já estiver instalado, ele permite selecionar volumes para a proteção. Caso contrário, o assistente instalará o software e protegerá todos os volumes. Configura uma programação padrão de proteção ou permite configurar uma programação personalizada. Nas definições avançadas, é possível escolher (ou criar) um repositório e estabelecer a criptografia para os dados protegidos.
Assistente de proteção de diversas máquinas	Botão Proteção em massa (guia Inicial)	Configura a proteção em várias máquinas que você especifica, a partir de um servidor de domínio do Active Directory do Windows, um host virtual do VMware vCenter Server/ESX(i) ou manualmente (inserindo uma lista em um formato especificado).

Tabela 1.

Nome do assistente	Iniciado por	Descrição
Assistente de replicação	Link Adicionar core de destino (guia Replicação)	Configura a replicação a partir de um core primário (ou de origem) para que uma cópia dos dados protegidos esteja sempre disponível em um core de destino separado.
Assistente de restauração de máquina	Botão Restaurar (barra de botões)	Orienta você durante o processo de restaurar dados a partir de um ponto de recuperação no Core para uma máquina protegida, ou ao iniciar uma bare metal restore.
Assistente de exportação	Botão Exportar (barra de botões), link Adicionar (guia Standby virtual)	Exporta dados do ponto de recuperação de uma máquina protegida para uma máquina virtual em qualquer formato de VM suportado. É possível realizar uma exportação única ou configurar o standby virtual para a exportação contínua.

Normalmente, os assistentes instalam ou configuram recursos no AppAssure, mas é possível modificar posteriormente a maioria desses aspectos no Core Console.

2

Instalação do AppAssure

Este capítulo descreve como instalar os componentes que você precisará para usar o AppAssure. Os seguintes tópicos estão incluídos:

- Entender os componentes do AppAssure
- Requisitos para instalação
- Instalação do AppAssure
- Instalação do AppAssure Core
- Instalação do software do AppAssure Agent
- Instalação do AppAssure Central Management Console
- Configuração do AppAssure Central Management Console
- Instalação automática de atualizações
- Desinstalação do software do AppAssure Agent
- Desinstalação do AppAssure Core
- Desinstalação do AppAssure Central Management Console

Antes de instalar o AppAssure, considere os componentes necessários para a sua implementação. Como requisito básico, planeje instalar o AppAssure Core em um servidor Windows dedicado, e o software do AppAssure Agent em cada máquina com Windows ou Linux que deseje proteger no core. Outros componentes também podem ser necessários.

Entender os componentes do AppAssure

Esta seção descreve os componentes do AppAssure disponíveis para cópia de segurança, replicação e recuperação após desastres. O propósito desta seção é ajudá-lo a entender os componentes que você poderá instalar no seu ambiente do AppAssure e como eles funcionarão juntos para ajudar a proteger seus dados.

- **AppAssure Core**: o componente central da arquitetura do AppAssure. O AppAssure Core fornece os serviços essenciais para cópia de segurança, recuperação, retenção, replicação, arquivamento e gerenciamento. Ele armazena e gerencia os dados de cópia de segurança de suas máquinas protegidas. O AppAssure Core é instalado em um servidor Windows dedicado. Dependendo de sua licença e dos requisitos do seu ambiente, pode ser preciso instalar diversos cores.
- **AppAssure Core Console**: um console baseado na Web usado para gerenciar um AppAssure Core individual e as máquinas protegidas e replicadas associadas. O Core installer automaticamente instala o software AppAssure Core Console.
- **AppAssure Central Management Console**: um portal de gerenciamento de vários cores, que simplifica o processo de gerenciar diversos AppAssure Cores. Com o Central Management Console em um servidor Windows, você pode agrupar e gerenciar vários Cores no seu ambiente usando uma única interface baseada na Web. Se você instalar diversos AppAssure Cores, é necessário instalar esse serviço separado para gerenciá-los.
- **AppAssure Agent**: o software e os serviços do Agent que possibilitam proteger seus dados. Você deverá instalar o software do Agent nas máquinas operando com Windows ou Linux em seu ambiente (por exemplo, em um Exchange Server, SQL Server, Linux server, etc.). Depois de adicionar uma máquina com o software Agent como uma máquina protegida no AppAssure Core, o software Agent rastreia os blocos

de dados alterados no volume de disco da máquina e cria imagens de snapshot dos dados, que envia ao Core com base no programa de cópia de segurança. Você gerencia as máquinas protegidas usando o Console do Core para o Core associado, incluindo estabelecer ou alterar a frequência das cópias de segurança.

- **Core de destino para replicação**: Para redundância, é possível replicar informações de snapshots de máquinas protegidas no AppAssure Core. Para isso, é preciso instalar o software AppAssure Core em um servidor Windows adicional. O segundo Core costuma estar localizado em um site físico diferente. No primeiro core (origem), você então configura a replicação no segundo core (destino), escolhendo que máquinas protegidas replicar e quando. Para obter mais informações sobre a replicação, consulte o *Guia do usuário do Dell AppAssure*.
- **Máquina virtual de standby virtual**: o AppAssure permite exportar seus dados para uma máquina virtual de standby virtual, o que fornece uma cópia de alta disponibilidade dos dados. Se estiver usando standby virtual, quando uma máquina protegida ficar inoperável, será possível inicializar a máquina virtual para realizar a recuperação. Se você planeja exportar dados para uma máquina virtual, uma plataforma de virtualização suportada, como VMware Workstation, VMware ESX(i), Microsoft Hyper-V ou Oracle VirtualBox, é necessária. Para obter mais informações sobre a configuração de uma máquina standby virtual, consulte o *Guia do usuário do Dell AppAssure*.

Requisitos para instalação

Esta seção descreve os requisitos de sistemas e licenças para a instalação dos componentes AppAssure Core, AppAssure Agent e AppAssure Central Management Console.

Infraestrutura de rede recomendada

Há uma década, a infraestrutura de backbone padrão apresentava velocidades de 100 megabits por segundo. As demandas por entradas/saídas e tráfego de rede aumentaram de forma contínua e substancial. Como resultado, os padrões para os backbones de rede aumentaram para atender a essa demanda. Os backbones de rede modernos suportam velocidades como gigabit Ethernet (GbE ou 1 GigE), que transfere quadros Ethernet a uma velocidade de 1 gigabit por segundo, ou 10 GigE, que é 10 vezes mais rápido.

A Dell recomenda que as organizações usem um backbone de pelo menos 1 GigE para um desempenho eficiente ao usar o AppAssure, e redes de 10 GigE para ambientes robustos. Redes de 10 GigE também são recomendadas ao proteger servidores com grandes volumes (5 TB ou mais).

Se houver diversas NICs (Network Interface Cards) na máquina core com suporte a agrupamento de NIC (junção de várias NICs físicas em uma única NIC lógica), e se os comutadores na rede permitirem, o uso do agrupamento de NIC no core pode fornecer desempenho extra. Nesses casos, agrupar placas de rede sobressalentes com suporte a agrupamento de NIC em qualquer máquina protegida, quando possível, também pode aumentar o desempenho geral.

Se o core usar iSCSI ou NAS (Network Attached Storage), a Dell recomenda usar placas NIC separadas para armazenamento e tráfego de rede, respectivamente.

Essas sugestões são baseadas nas necessidades típicas de uma infraestrutura de rede para suportar todas as operações de negócios, além dos recursos de cópia de segurança, replicação e recuperação fornecidos pelo AppAssure.

Suporte a UEFI e ReFS

A Interface Unificada de Firmware Extensível (UEFI) substitui o Sistema Básico de Entrada/Saída (BIOS) e é usada nos sistemas operacionais Windows 8, Windows 8.1, Windows Server 2012 e Windows Server 2012 R2. A UEFI utiliza as partições do sistema da Interface de Firmware Extensível (EFI), que são processadas como volumes FAT32 simples. Recursos de proteção e recuperação estão disponíveis no AppAssure para partições de sistema da EFI. O AppAssure também suporta a proteção e recuperação de volumes de Sistema de Arquivos Resilientes (ReFS) para o Windows Server 2012 e 2012 R2.

Limitações de suporte para volumes dinâmicos e básicos

O AppAssure suporta a obtenção de snapshots de todos os volumes dinâmicos e básicos. O AppAssure também suporta a exportação de volumes dinâmicos simples que estão em um único disco físico. Como o próprio nome indica, os volumes dinâmicos simples não são volumes distribuídos, espelhados ou estendidos.

Discos dinâmicos (com exceção de discos dinâmicos simples, conforme descrito anteriormente) não estão disponíveis para seleção no Assistente de exportação. Volumes dinâmicos não simples têm geometrias de disco arbitrárias, que não podem ser totalmente interpretadas. Logo, o AppAssure não suporta a exportação de volumes dinâmicos complexos ou não simples.

Uma notificação aparece na interface do usuário para alertar que as exportações são limitadas e estão restritas a volumes dinâmicos simples. Se você tentar exportar algo que não seja um volume único simples, o trabalho de exportação falhará.

Requisitos do sistema do AppAssure

Instale o AppAssure Core em um servidor Windows 64 bits dedicado. Para cada máquina que desejar proteger em um AppAssure Core, instale a versão do software do AppAssure Agent adequada ao sistema operacional da máquina. Dependendo de sua licença e dos requisitos do seu ambiente, pode ser preciso instalar diversos cores, cada um em um servidor dedicado. E, opcionalmente, para o gerenciamento remoto de diversos cores, você pode instalar o AppAssure Central Management Console em um computador Windows de 64 bits.

Antes de instalar o AppAssure 5.4.3, verifique se seu sistema atende aos seguintes requisitos mínimos de hardware e software. Para obter mais orientações sobre dimensionamento de seu hardware, software, memória, armazenamento e requisitos de rede, consulte o Dell AppAssure artigo da base de conhecimento 118407, "Dimensionando implantações do AppAssure."

△ **CUIDADO: A Dell não suporta a execução do AppAssure Core em sistemas operacionais Windows Core, os quais oferecem funções de servidor limitadas. Isso inclui todas as edições do Windows Server 2008 Core, Windows Server 2008 R2 Core, Windows Server 2012 Core e Windows Server 2012 R2 Core. Três desses sistemas operacionais edição Core *são* suportados para a execução do software AppAssure Agent.**

CUIDADO: A Dell não recomenda a execução do AppAssure Core na mesma máquina física que atua como o host do Hyper-V. (Essa recomendação não se aplica a appliances de cópia de segurança e recuperação da Dell).

AppAssure requisitos do Core e do Central Management Console

Tabela 2. AppAssure requisitos do Core e do Central Management Console

Requisito	Detalhes
Sistema operacional	O AppAssure Core não suporta sistemas de 32 bits e sistemas Linux. O AppAssure Core necessita de um dos seguintes sistemas operacionais (OS) do Windows x64: • Microsoft Windows 7 • Microsoft Windows 8, 8.1* • Microsoft Windows Server 2008,2008 R2 (**exceto** edições Core) • Microsoft Windows Server 2012, 2012 R2* (**exceto** edições Core) NOTA: Os sistemas operacionais Windows requerem que o .NET Framework 4.0x esteja instalado para executar o serviço AppAssure Core. Além disso, os sistemas operacionais marcados com * exigem a função/recurso ASP .NET 4.5x. Ao instalar ou atualizar o AppAssure Core, o instalador irá verificar esses componentes com base no OS do servidor Core e irá instalá-los ou ativá-los automaticamente, se necessário. O AppAssure Core suporta todas as edições x64 dos OS do Windows listados. a menos que indicado diferentemente. O AppAssure Core não suporta edições Windows Server Core. O AppAssure Core suporta o sistema operacional base para cada OS listado, bem como o OS atualizado para qualquer pacote de serviços disponível, a menos que indicado diferentemente. Para obter um desempenho ideal, recomenda-se instalar o AppAssure Core no Windows 8.1 (ou mais recente) e Windows Server 2012 (ou mais recente).
Arquitetura	Somente 64 bits
Memória	8 GB ou mais de memória RAM NOTA: A Dell recomenda o uso da memória ECC (Verificação e correção de erros) para garantir o desempenho ideal dos servidores do AppAssure Core.
Processador	Quad-core ou superior
Armazenamento	Armazenamento por conexão direta, Rede de área de armazenamento ou Armazenamento conectado à rede
Rede	Mínimo de 1 GB de Ethernet (GbE) NOTA: A Dell recomenda backbone de rede de 10GbE para ambientes robustos.

AppAssure Requisitos do software Agent

Tabela 3. AppAssure Requisitos do software Agent

Requisito	Detalhes
	O software AppAssure Agent suporta sistemas operacionais de 32 e 64 bytes do Windows e Linux, incluindo: • Microsoft Windows XP SP3 (Professional Edition apenas) • Microsoft Windows Vista • Microsoft Windows 7 • Microsoft Windows 8, 8.1* • Microsoft Windows Server 2003, 2003 R2 • Microsoft Windows Server 2008, 2008 R2 (todas as edições, exceto Windows Server 2008 Core) • Microsoft Windows Server 2012, 2012 R2* • Red Hat Enterprise Linux (RHEL) 6.3, 6.4, 6.5, 6.6, 7 (x64) • CentOS Linux 6.3, 6.4, 6.5, 6.6, 7 (x64) • Ubuntu Linux 12.04 LTS, 13.04, 14.04 • SUSE Linux Enterprise Server (SLES) 11 (SP2 e posterior)
	NOTA: Os sistemas operacionais Windows requerem que o Microsoft .NET Framework (4.0x) esteja instalado para executar o serviço AppAssure Agent. Além disso, os sistemas operacionais marcados com * exigem a função/recurso ASP .NET 4.5x. Ao instalar ou atualizar o software do AppAssure Agent, o instalador irá verificar esses componentes e irá instalá-los ou ativá-los automaticamente, se necessário. O software AppAssure Agent suporta todas as edições dos OS do Windows listadas. a menos que indicado diferentemente. Somente a Professional Edition do Windows XP é suportada. O software AppAssure Agent suporta o sistema operacional base para cada OS listado, bem como o OS atualizado para qualquer pacote de serviços disponível, a menos que indicado diferentemente. Máquinas protegidas operando com Windows XP devem estar usando o SP3. O software AppAssure Agent suporta a instalações da edição Windows Server Core para o Windows 2008 R2, 2012 e 2012 R2. Somente para o Windows Server 2008 R2 Core, você deve possuir SP1 ou uma versão mais recente. A edição Windows Server 2008 Core não é suportada. O software AppAssure Agent suporta as distribuições do Linux incluídas na lista. A maioria das versões lançadas do kernel foram testadas. Somente os sistemas de arquivo ext3, ext4 e xfs são suportados. Agents instalados no Microsoft Hyper-V Server 2012 funcionam no modo de edição do Core do Windows Server 2012. NOTA: A cópia de segurança nativa do Cluster Shared Volumes é suportada somente nas máquinas protegidas do Windows 2008 R2.
Arquitetura	32 bits ou 64 bits
Memória	4 GB ou superior
Suporte do Microsoft Exchange	Microsoft Exchange 2007 SP1 Rollup 5 ou mais recente, Microsoft Exchange 2010 ou Microsoft Exchange 2013
Suporte Microsoft SQL	Microsoft SQL Server 2005 ou mais recente
Armazen-amento	Armazenamento por conexão direta, Rede de área de armazenamento ou Armazenamento conectado à rede
Rede	Mínimo de 1 GB de Ethernet (GbE) NOTA: A Dell recomenda backbone de rede de 10GbE para ambientes robustos.

Para obter mais informações sobre como usar o AppAssure, consulte o *Guia do usuárioDell AppAssure*. Para obter mais informações sobre o gerenciamento de Dell AppAssurelicenças, consulte o *Portal de licenças do Dell AppAssure Guia do usuário*. Para obter mais informações sobre dimensionamento de seu hardware, software, memória, armazenamento e requisitos de rede, consulte o artigo da base de conhecimentoDell AppAssure 118407, "Dimensionando implantações do AppAssure."

Requisitos de licença

Antes que possa instalar os componentes do AppAssure, você precisa se registrar no Portal de licenças do Dell AppAssure, criar uma conta e obter uma chave ou arquivo de licença, que é necessário para baixar o software AppAssure Core e AppAssure Agent e para configurar e proteger máquinas.

Para obter mais informações sobre o Portal de licenças do Dell AppAssure, sobre como obter uma chave de licença e registrar-se para uma conta, consulte o Guia do usuário do *Portal de licenças do Dell AppAssure*.

Instalação do AppAssure

A instalação do AppAssure envolve instalar o AppAssure Core em suas máquinas servidor Windows dedicadas e os serviços do AppAssure Agent nas máquinas que você deseja proteger, que podem estar usando Windows ou Linux. Caso você for configurar e gerenciar diversos cores, também será necessário instalar o serviço AppAssure Central Management Console.

As etapas que você precisa seguir para instalar o AppAssure são:

- **Etapa 1:** Registre-se em Portal de licenças do Dell AppAssure em https://licenseportal.com, crie uma conta e obtenha uma licença de software. Uma chave ou arquivo de licença é necessário para baixar o AppAssure Core e do software AppAssure Agent, assim como para configurar e proteger as máquinas. Para obter mais informações sobre como obter uma chave ou arquivo de licença ou registrar-se e criar uma conta do Portal de licenças do Dell AppAssure, consulte o *Guia do usuário do Portal de licenças do Dell AppAssure*.
- **Etapa 2:** Examine e certifique-se de que os requisitos do sistema foram atendidos para os servidores e máquinas nos quais você instalará os componentes do AppAssure. Para obter mais informações, consulte Requisitos para instalação.
- **Etapa 3:** Instale o software AppAssure Core nas máquinas operando com Windows que você usará como Cores. Para obter mais informações, consulte Instalação do AppAssure Core.
- **Etapa 4:** Instale o software AppAssure Agent nas máquinas operando com Windows ou Linux que serão protegidas. Para obter mais informações, consulte Instalação do software do AppAssure Agent em máquinas com Windows e Instalação do software do Agent em máquinas com Linux.
- **Etapa 5:** Se você precisar gerenciar vários AppAssure Cores em seu ambiente, é preciso instalar e configurar o AppAssure Central Management Console. Para obter mais informações sobre a instalação do Central Management Console, consulte Instalação do AppAssure Central Management Console. Para obter mais informações sobre a configuração do Central Management Console, consulte Configuração do AppAssure Central Management Console.

NOTA: Depois de ter instalado todos os componentes necessários, você precisa criar um repositório e definir locais de armazenamento para seus dados protegidos. Você pode fazer isso como um processo separado ou como parte do fluxo de trabalho ao usar o Assistente de proteção de máquina.

Como opção, você pode desejar realizar outras tarefas de configuração, como definir chaves de criptografia, configurar notificação de eventos ou replicar pontos de recuperação de um core de origem para um core de destino. Cada uma dessas tarefas de configuração é incluída no recurso Guia de início rápido descrito no *Guia do usuário do Dell AppAssure*. Para obter mais informações sobre essas tarefas, bem como configurar um server de SMTP para mensagens de notificação, alterar a política de retenção de dados ou configurar a capacidade de anexação do SQL, consulte o *Guia do usuário do Dell AppAssure*.

Instalação do AppAssure Core

Como o AppAssure Core armazena e gerencia as cópias de segurança de todas as máquinas protegidas do seu ambiente, você deve instalar o AppAssure Core em um servidor dedicado. Dependendo de sua licença e dos requisitos do seu ambiente, pode ser preciso instalar diversos cores.

Para instalar o AppAssure Core, você precisa fazer login no Portal de licenças do Dell AppAssure em https://licenseportal.com, registrar uma conta e, em seguida, baixar o instalador e obter uma chave de licença ou arquivo de licença para ativar o software. Para obter mais informações, consulte o *Guia do usuário do Portal de licenças do Dell AppAssure*.

O Portal de licenças do Dell AppAssure identifica um AppAssure Core por seu ID de Core. Por esse motivo, para evitar um conflito entre IDs do Core de gerenciamento, a Dell recomenda não clonar máquinas com o AppAssure Core instalado. No caso de você já ter feito isso, remova o software AppAssure Core da máquina clonada e reinstale-o. Isso resulta na designação de um novo ID do Core à máquina clonada.

Ao instalar o AppAssure Core, você pode optar por atualizar automaticamente o software AppAssure Core. Você também pode optar por receber notificações sobre as atualizações ou ignorá-las. Após a conclusão da instalação, as definições podem ser alteradas a qualquer momento. Para obter mais informações sobre a alteração das definições de atualização automática, consulte o tópico Configuração das definições de atualização no *Guia do usuário do Dell AppAssure*.

> **NOTA:** Para obter um desempenho ideal, recomenda-se instalar o AppAssure Core no Windows 8.1 ou Windows Server 2012 R2.
>
> O AppAssure Core exige o uso de uma plataforma de 64 bits do Windows. Sistemas de 32 bits e sistemas Linux não são suportados. Para obter mais informações, consulte Requisitos do sistema do AppAssure. Além disso, nos sistemas operacionais Windows 8, Windows 8.1, Windows Server 2012 e Windows Server 2012 R2, você precisa ter o recurso ASP.NET 4.5 instalado no servidor. Caso você não tenha o recurso instalado, a GUI não será carregada corretamente.

Após a instalação do AppAssure Core, você pode baixar o AppAssure Agent installer a partir do Core ou do Portal de licenças do Dell AppAssure para cada máquina que será protegida pelo Core.

Para obter mais informações sobre o AppAssure Agent Installer e sobre a instalação do software Agent em máquinas com Windows, consulte Instalação do software do AppAssure Agent em máquinas com Windows. Para obter informações sobre a instalação do software Agent em máquinas com Linux, consulte Instalação do software do Agent em máquinas com Linux.

Execute o procedimento abaixo para instalar o AppAssure Core.

Para instalar o AppAssure Core

1. Baixe o arquivo do AppAssure Core installer no Portal de licenças do Dell AppAssure, por exemplo:

   `Core-X64-5.x.x.xxxxx.exe`

2. Clique em **Executar** para iniciar o instalador.

   > **NOTA:** O instalador verifica se o .NET Framework 4.0 está instalado no seu sistema. Caso ausente, o instalador solicitará que você baixe e instale o Framework.

3. A caixa de diálogo Instalação aparece. No campo de idioma, selecione o idioma adequado e clique em OK.

   O instalador prepara a instalação e então o Assistente de instalação do AppAssure Core aparece.

4. No Assistente de instalação do AppAssure Core, na página Bem-vindo, clique em Avançar para prosseguir com a instalação.

   A página Acordo de licença é exibida.

5. Clique em **Eu aceito os termos do acordo de licença** e, em seguida, clique em **Avançar**.

   A página Pré-requisitos é exibida.

6 O AppAssure Core Installer confirma a existência dos arquivos de pré-requisitos.
   - Se os pré-requisitos não existirem, o AppAssure Agent Installer identifica quais são os arquivos necessários e exibe os resultados de acordo. Clique em **Instalar pré-requisitos**.
   - Se os arquivos de pré-requisitos existirem, uma mensagem será exibida indicando que todos os pré-requisitos estão instalados na máquina.
7 Quando a instalação dos pré-requisitos for concluída, clique em **Avançar**.
8 Na página Opções de instalação, revise as opções de instalação. Caso necessário, modifique-as conforme descrito abaixo.
   - No campo de texto Pasta de destino, revise a pasta de destino para a instalação. Caso queira alterar o local, faça o seguinte:
     - Clique no ícone de pasta.
     - Na caixa de diálogo Navegar até a pasta de destino, selecione um novo local.
     - Clique em **OK**.
   - No campo de texto Número da porta, insira o número da porta que será usada para a comunicação entre o software Agent na máquina protegida e o AppAssure Core.

     NOTA: O valor padrão é *8006*. Se você alterar o número da porta, certifique-se de tomar nota do número para caso futuramente precise alterar as definições de configuração.
   - Como opção, na área Selecionar componentes adicionais, se desejar instalar o Mailbox Restore, selecione **Mailbox Restore**.

     O Mailbox Restore for Microsoft Exchange é um programa abrangente de recuperação de e-mails, que funciona com o AppAssure e com o Local Mount Utility (LMU) do AppAssure para recuperar itens do Exchange, desde um armazenamento de dados completo até uma única mensagem de e-mail. Para obter mais informações sobre o Mailbox Restore, consulte o *Guia do usuário do Mailbox Restore for Microsoft Exchange usando o AppAssure*.
   - Selecione **Permitir que o Core envie automaticamente diagnósticos e informações do usuário para o software DellAppAssure** para enviar diagnósticos e informações do usuário para a Dell. Caso não queira enviar as informações, desmarque a opção.
9 Quando estiver satisfeito com as opções de instalação, clique em **Avançar**.

   A página Opções de atualização é exibida.
10 Na página Opções de atualização, selecione uma das seguintes opções:

Tabela 4.

Opção	Descrição
Instalar atualizações automaticamente (recomendado)	Se você selecionar essa opção, o AppAssure Core automaticamente comparará sua versão do Core com a versão mais recente disponível, uma vez por semana. Se houver uma atualização disponível, a versão atualizada é instalada depois da conclusão dos trabalhos noturnos.
Notificar-me sobre atualizações, mas não instalá-las automaticamente	Se você selecionar esta opção, um alerta na parte superior do AppAssure Core Console será exibido quando uma nova versão estiver disponível, incluindo um link para baixar essa atualização.
Nunca procurar por atualizações	Caso selecione esta opção, você não será notificado quando uma nova versão estiver disponível.

Se você optar por instalar atualizações automáticas ou ser notificado sobre elas, a versão do software no AppAssure Core é verificada com relação às atualizações de software regularmente. Se uma nova versão for detectada, e se você tiver selecionado a opção de atualizar automaticamente, a versão atualizada do Core é instalada depois da conclusão de outros trabalhos noturnos.

NOTA: A Dell recomenda usar a opção de atualização automática. A configuração padrão das atualizações automáticas é verificar semanalmente se há atualizações.

É possível alterar a frequência com que o sistema verifica as atualizações (as opções incluem diariamente, semanalmente, mensalmente ou nunca) a qualquer momento alterando as definições de atualização do Core na guia Configuração do AppAssure Core Console. Para obter mais informações sobre como alterar as definições, consulte o tópico Configuração das definições de atualização no *Guia do usuário do Dell AppAssure*.

11 Quando estiver satisfeito com as opções de atualização, clique em **Instalar**.

A página Progresso é exibida e inclui uma barra de status, que permite monitorar o progresso da instalação.

Quando a instalação for concluída, a página Concluído será exibida.

12 Clique em **Concluir** para fechar o instalador.

> **NOTA:** Na primeira vez em que você abrir o AppAssure Core, será preciso inserir a sua chave de licença.

Ao concluir a instalação do AppAssure Core, você terá que instalar o software do Agent para proteger suas máquinas com Windows ou Linux. Para obter mais informações, consulte Instalação do AppAssure.

Para obter informações sobre a configuração do AppAssure Core e sobre a proteção e o gerenciamento dos seus dados, consulte o *Guia do usuário do Dell AppAssure*.

Instalação do software do AppAssure Agent

Instale o software AppAssure Agent em todas as máquinas do seu ambiente que serão protegidas pelo AppAssure Core.

> **NOTA:** É preciso reiniciar o sistema para concluir a instalação ou o upgrade do software do AppAssure Agent.

Revise os métodos para obter o software AppAssure Agent e determinar que método você irá usar. Então obtenha o software e instale nas máquinas que deseja proteger no AppAssure Core. Por fim, adicione as máquinas para proteção no seu Core.

Esta seção inclui os seguintes tópicos:

- Obtenção do software do AppAssure Agent
- Instalação do software do AppAssure Agent em máquinas com Windows
- Instalação do software do Agent em máquinas com o Windows Server Core Edition
- Instalação do software do Agent em máquinas com Linux

Obtenção do software do AppAssure Agent

Obtenha o software Agent usando um dos seguintes métodos:

- **Download no AppAssure Core Console.** Se o AppAssure Core estiver instalado, você pode acessar o AppAssure Core Console e baixar o software na máquina que deseja proteger. Selecione **Downloads** na guia Ferramentas e, em seguida, baixe o instalador Web para o componente Agent.

  Para obter mais informações sobre a instalação do Core, consulte Instalação do AppAssure Core.

- **Download no Portal de licenças.** Se você já registrou o seu software no Portal de licenças do Dell AppAssure, pode efetuar login no Portal de licenças em https://licenseportal.com e baixar o software para a máquina que deseja proteger.

  Para obter mais informações sobre o Portal de licenças do Dell AppAssure, incluindo como obter uma chave de licença ou registrar-se e criar uma conta do Portal de licenças, consulte o Guia do usuário do *Portal de licenças do Dell AppAssure*.

- **Implementar o software do Agent ao proteger uma máquina.** Se o AppAssure Core estiver instalado, você pode implementar o software do Agent na máquina que deseja proteger usando o Assistente de proteção de máquina. Para obter mais informações sobre a forma de uso desse assistente, consulte o tópico Proteção de uma máquina no *Guia do usuário do Dell AppAssure*.
- **Implementar o software do Agent ao proteger diversas máquinas.** Se o AppAssure Core estiver instalado, você pode implementar o software do Agent em diversas máquinas usando o Assistente de proteção de diversas máquinas. Para obter mais informações sobre a forma de uso desse assistente, consulte o tópico Proteção de várias máquinas no *Guia do usuário do Dell AppAssure*.
- **Usar o recurso Implantação em massa.** Se o AppAssure Core estiver instalado, você pode implementar o software do Agent em diversas máquinas usando o recurso de implementação em massa, que pode ser acessado na guia Ferramentas do AppAssure Core Console. Para obter mais informações sobre a forma de uso do recurso implementação em massa, consulte o tópico Implementação em várias máquinas no *Guia do usuárioDell AppAssure*.

Instalação do software do AppAssure Agent em máquinas com Windows

Implemente o arquivo do AppAssure Agent Installer na máquina que deseja proteger usando um dos métodos descritos em Instalação do software do AppAssure Agent. Então inicie o programa do instalador conforme descrito abaixo para instalar o software em todas as máquinas com Windows que deseje proteger no AppAssure Core.

> **NOTA:** Você precisa executar o instalador com privilégios de administrador local.
>
> O procedimento para instalação em edições do Windows Server Core difere de outras versões do Windows, uma vez que essa versão descreve como instalar a partir da linha de comandos. Para obter mais informações, consulte Instalação do software do Agent em máquinas com o Windows Server Core Edition.

Para instalar o software do Agent em máquinas com Windows

1. Na máquina que você deseja proteger, clique duas vezes no arquivo do AppAssure Agent installer.
2. Na caixa de diálogo Abrir arquivo - Aviso de segurança, clique em Executar.
3. A caixa de diálogo Instalação aparece. No campo de idioma, selecione o idioma adequado e clique em OK.

   O instalador prepara a instalação.
4. Se a máquina tiver uma versão anterior do software AppAssure Agent instalada, uma mensagem será exibida perguntando se você deseja fazer a atualização para a versão atual. Clique em Sim para ir para Etapa 7.

   Se essa for a primeira vez que o software AppAssure Agent está sendo instalado na máquina, prossiga para Etapa 5.
5. No Assistente de instalação do AppAssure Agent, na página Bem-vindo, clique em **Avançar** para prosseguir com a instalação.

   A página Acordo de licença é exibida.
6. Na página Acordo de licença, clique em **Eu aceito os termos do acordo de licença** e, em seguida, clique em **Avançar**.

   A página Pré-requisitos é exibida.
7. O AppAssure Agent Installer confirma a existência dos arquivos de pré-requisitos.
   - Se os arquivos de pré-requisitos existirem, uma mensagem será exibida indicando que todos os pré-requisitos estão instalados na máquina.
   - Se os arquivos de pré-requisitos não existirem, o AppAssure Agent Installer identificará quais são os arquivos necessários e exibirá os resultados de acordo; por exemplo, Microsoft .NET Framework 4.0 ou Microsoft System CLR Types para SQL Server 2008 R2 (x64). Clique em **Instalar pré-requisitos**.

8 Quando a instalação dos pré-requisitos for concluída, clique em **Avançar**.

   A página Opções de instalação é exibida.

9 Na página Opções de instalação, revise as opções de instalação. Caso necessário, modifique-as conforme descrito abaixo.

   - No campo de texto Pasta de destino, revise a pasta de destino para a instalação. Caso queira alterar o local, faça o seguinte:
     - Clique no ícone de pasta.
     - Na caixa de diálogo Navegar até a pasta de destino, selecione um novo local.
     - Clique em **OK**.
   - No campo de texto Número da porta, insira o número da porta que será usada para a comunicação entre o software Agent na máquina protegida e o AppAssure Core.

     NOTA: O valor padrão é *8006*. Se você alterar o número da porta, certifique-se de tomar nota do número para caso futuramente precise alterar as definições de configuração.

   - Selecione **Permitir que o Agent envie automaticamente diagnósticos e informações do usuário para o softwareDellAppAssure** para enviar diagnósticos e informações do usuário para a Dell. Caso não queira enviar as informações, desmarque a opção.

10 Quando estiver satisfeito com as opções de instalação, clique em **Instalar**.

   A página Progresso é exibida e inclui uma barra de status, que permite monitorar o progresso da instalação.

   Quando a instalação for concluída, a página Concluído será exibida. Vá para Etapa 12.

11 Se estiver realizando o upgrade de uma versão anterior do AppAssure Agent, o Assistente de instalação do AppAssure Agent aparece. Na página de progresso, você pode ver o progresso da instalação.

   Quando a instalação for concluída, a página Concluído será exibida.

12 Na página Concluído, você vê uma mensagem indicando que o sistema deve ser reiniciado antes de a instalação entrar em vigor. Realize uma das seguintes ações e clique em Concluir:

   - Para reiniciar agora, selecione Sim, desejo reiniciar meu computador agora.
   - Para reiniciar mais tarde, desmarque a opção **Sim, desejo reiniciar meu computador agora.**

Instalação do software do Agent em máquinas com o Windows Server Core Edition

Execute as etapas do procedimento a seguir para instalar o software do Agent em uma máquina com Windows Server Core.

NOTA: O procedimento a seguir instala o software do Agent em modo console. Para instalar em modo silencioso, adicione `/silent` ao nome do arquivo do instalador na linha de comando. Por exemplo, `Agent-X64-5.X.X.xxxxx.exe /silent`.

Para instalar o software Agent em máquinas com o Windows Server Core Edition

1 Baixe o arquivo do AppAssure Agent installer no Portal de licenças do Dell AppAssure ou no AppAssure Core.

2 Em um prompt de comando, vá para o diretório onde se encontra o arquivo do AppAssure Agent installer e insira o nome do arquivo do instalador para dar início à instalação:

```
Agent-X64-5.x.x.xxxxx.exe
```

   O programa de instalação instala o software Agent e exibe o progresso no console. Após a conclusão, novas instalações ativarão uma reinicialização automática da máquina, enquanto que atualizações do Agent podem não precisar de uma reinicialização.

Instalação do software do Agent em máquinas com Linux

As instruções de instalação do software Agent em uma máquina com Linux são um pouco diferentes dependendo da distribuição do Linux que você está usando. Para obter mais informações sobre a preparação e instalação do agente no Linux, consulte as seguintes seções:

- Antes de começar
- Instalação do software do Agent em Ubuntu
- Instalação do software do Agent em Red Hat Enterprise Linux e CentOS
- Instalação do software do Agent no SUSE Linux Enterprise Server
- Início e interrupção do Daemon do Agent para Linux
- Execução de scripts no Agent para Linux

Antes de começar

Ao instalar o software Agent em uma máquina Linux, seja pela primeira vez ou ao atualizar de uma versão diferente, é preciso reiniciar a máquina depois de concluir a instalação. Reiniciar garante que a versão do driver de kernel adequada seja usada para proteger a máquina.

Consulte as seguintes informações importantes antes de começar a instalação do Agent no Linux.

- Baixar a distribuição do Linux
- Sobre a segurança
- Configuração do firewall
- Localização dos arquivos do Agent para Linux
- Dependências do Agent

Baixar a distribuição do Linux

É necessário baixar o instalador de 32 ou 64 bits específico da distribuição em todos os servidores Linux que você deseja proteger. É possível baixar os instaladores no Portal de licenças do Dell AppAssure em https://licenseportal.com. Para obter mais informações, consulte o *Guia do usuário do portal de licenças do Dell AppAssure*.

Sobre a segurança

A segurança em torno da proteção de uma máquina está baseada no Módulo de autenticação conectável (PAM) do Linux. Depois que um usuário é autenticado através de libpam, o usuário só tem autorização para proteger a máquina se estiver em um dos seguintes grupos: sudo, admin, appassure ou wheel. Para obter mais informações sobre a proteção de uma máquina, consulte a seção "Proteção de uma máquina" no *Guia do usuário do Dell AppAssure*.

Configuração do firewall

A instalação do Agent para Linux substituiu quaisquer regras de firewall que não foram aplicadas através de UFW, Yast2 ou system-config-firewall. Se você adicionou manualmente regras de firewall, será preciso adicionar portas do AppAssure após a instalação. Uma cópia de segurança das regras existentes será gravada em:

```
/var/lib/appassure/backup.fwl
```

É necessário adicionar exceções de firewall para todos os servidores executando o AppAssure Agent para as portas TCP 8006 e 8009 para que o AppAssure Core tenha acesso aos agentes.

Localização dos arquivos do Agent para Linux

Os arquivos do agente para Linux estarão localizados nos seguintes diretórios para todas as distribuições:

- mono:

  ```
  /opt/appassure/mono
  ```

- agent:

  ```
  /opt/appassure/aagent
  ```

- aamount:

  ```
  /opt/appassure/amount
  ```

- aavdisk e aavdctl:

  ```
  /usr/bin
  ```

- arquivos de configuração para aavdisk:

  ```
  /etc/appassure/aavdisk.conf
  ```

- wrappers para aamount e agent:

  ```
  /usr/bin/aamount
  /usr/bin/aagent
  ```

- scripts de execução automática para aavdisk e agent:

  ```
  /etc/init.d/appassure-agent
  /etc/init.d/appassure-vdisk
  ```

Dependências do Agent

As seguintes dependências são necessárias e instaladas como parte do pacote do Agent installer:

- Para Ubuntu:
  - O appassure-vss exige:

    ```
    dkms, gcc, make, linux-headers-‘uname-r‘
    ```

  - O appassure-aavdisk exige:

    ```
    libc6 (>=2.7-18), libblkid1, libpam0g, libpcre3
    ```

  - O appassure-mono exige:

    ```
    libc6 (>=2.7-18)
    ```

- Para Red Hat Enterprise Linux e CentOS:
  - O nbd-dkms exige

    ```
    dkms, gcc, make, kernel-headers-‘uname-r‘ kernel-devel-‘uname-r‘
    ```

  - O appassure-vss exige:

    ```
    dkms, gcc, make, kernel-headers-‘uname-r‘ kernel-devel-‘uname-r‘
    ```

  - O appassure-aavdisk exige:

    ```
    nbd-dkms, libblkid, pam, pcre
    ```

  - O appassure-mono exige:

    ```
    glibc >=2.11
    ```

- Para SUSE Linux Enterprise Server:
  - O nbd-dkms exige:

    ```
    dkms, gcc, make, kernel-syms
    ```

  - O appassure-vss exige:

```
dkms, kernel-syms, gcc, make
```

- O appassure-aavdisk exige:

```
libblkid1, pam, pcre
```

- O appassure-mono exige:

```
glibc >= 2.11
```

Instalação do software do Agent em Ubuntu

Execute as etapas a seguir para instalar o AppAssure Agent no Ubuntu.

NOTA: Antes de realizar estas etapas, certifique-se que você fez o download do pacote do instalador específico do Ubuntu no diretório $HOME do usuário conectado no momento.

Para instalar o software Agent em Ubuntu

1 Abra uma sessão do terminal com acesso raiz.

2 Para tornar o AppAssure Agent installer executável, digite o seguinte comando:

```
chmod +x appassure-installer_ubuntu_amd64_5.x.x.xxxxx.sh
```

NOTA: Em ambientes de 32 bits, o instalador chama-se "`appassure-installer_ubuntu_i386_5.x.x.xxxxx.sh`".

3 Pressione **<Enter>**.

O arquivo se torna executável.

4 Para extrair e instalar o AppAssure Agent, digite o seguinte comando:

```
./appassure-installer_ubuntu_amd64_5.x.x.xxxxx.sh
```

5 Pressione **<Enter>**.

O Agent do Linux começa o processo de extração e instalação. Quaisquer pacotes ou arquivos ausentes exigidos pelo Agent serão baixados e instalados automaticamente como parte do script.

NOTA: Para obter informações sobre os arquivos exigidos pelo software Agent, consulte Dependências do Agent.

Após a conclusão do instalador, o software Agent estará em execução na sua máquina. Para obter informações sobre como proteger esta máquina com o Core, consulte o capítulo "Proteção de estações de trabalho e servidores" no *Guia do usuário do Dell AppAssure*.

Instalação do software do Agent em Red Hat Enterprise Linux e CentOS

Execute as etapas abaixo para instalar o software AppAssure Agent em Red Hat Enterprise e no CentOS.

NOTA: Antes de realizar estas etapas, certifique-se que você fez o download do pacote do instalador Red Hat ou CentOS no diretório $HOME do usuário conectado no momento. As seguintes etapas se aplicam a ambientes de 32 e 64 bits.

Para instalar o Agent no Red Hat Enterprise Linux e CentOS

1 Abra uma sessão do terminal com acesso raiz.

2 Para tornar o AppAssure Agent installer executável, digite o seguinte comando:

```
chmod +x appassure-installer__rhel_amd64_5.x.x.xxxxx.sh
```

NOTA: Em ambientes de 32 bits, o instalador chama-se "`appassure-installer__rhel_i386_5.x.x.xxxxx.sh`".

3 Pressione **<Enter>**.

   O arquivo se torna executável.

4 Para extrair e instalar o AppAssure Agent, digite o seguinte comando:

```
./appassure-installer_rhel_amd64_5.x.x.xxxxx.sh
```

5 Pressione **<Enter>**.

   O software Agent do Linux começa o processo de extração e instalação. Quaisquer pacotes ou arquivos ausentes exigidos pelo Agent serão baixados e instalados automaticamente como parte do script.

   NOTA: Para obter informações sobre os arquivos exigidos pelo software Agent, consulte Dependências do Agent.

Após a conclusão do instalador, o software Agent estará em execução na sua máquina. Para obter informações sobre como proteger esta máquina com o Core, consulte o capítulo "Proteção de estações de trabalho e servidores" no *Guia do usuário do Dell AppAssure*.

Instalação do software do Agent no SUSE Linux Enterprise Server

Execute as etapas abaixo para instalar o AppAssure Agent no SUSE Linux Enterprise Server (SLES).

NOTA: Antes de realizar estas etapas, certifique-se que você fez o download do pacote do instalador Red Hat ou CentOS no diretório $HOME do usuário conectado no momento. As seguintes etapas se aplicam a ambientes de 32 e 64 bits.

Para instalar o software Agent no SUSE Linux Enterprise Server

1 Abra uma sessão do terminal com acesso raiz.

2 Para tornar o AppAssure Agent installer executável, digite o seguinte comando:

```
chmod +x appassure-installer_sles_amd64_5.x.x.xxxxx.sh
```

   NOTA: Em ambientes de 32 bits, o instalador chama-se "`appassure-installer__sles_i386_5.x.x.xxxxx.sh`".

3 Pressione **<Enter>**.

   O arquivo se torna executável.

4 Para extrair e instalar o AppAssure Agent, digite o seguinte comando:

```
./appassure-installer_sles_amd64_5.x.x.xxxxx.sh
```

5 Pressione **<Enter>**.

   O Agent do Linux começa o processo de extração e instalação. Quaisquer pacotes ou arquivos ausentes exigidos pelo Agent serão baixados e instalados automaticamente como parte do script.

   Para obter informações sobre os arquivos exigidos pelo software Agent, consulte Dependências do Agent.

6 Quando solicitado a instalar os novos pacotes, digite "y" e pressione **<Enter>**.

   O sistema conclui o processo de instalação.

Após a conclusão do instalador, o software Agent estará em execução na sua máquina. Para obter informações sobre como proteger esta máquina com o Core, consulte a seção "Proteção de estações de trabalho e servidores" no *Guia do usuário do Dell AppAssure*.

Início e interrupção do Daemon do Agent para Linux

Você pode manualmente iniciar, interromper e visualizar o status do software Agent e do aavdisk em todas as distribuições suportadas usando os comandos padrão conforme a descrição nas seguintes tabelas, respectivamente.

Tabela 5.

Para iniciar o...	Use o seguinte comando...
serviço do agente	sudo /etc/init.d/appassure-agent start
aavdisk	sudo /etc/init.d/appassure-vdisk start

Tabela 6.

Para interromper o...	Use o seguinte comando...
serviço do agente	sudo /etc/init.d/appassure-agent stop
aavdisk	sudo /etc/init.d/appassure-vdisk stop

Tabela 7.

Para visualizar o status do...	Use o seguinte comando...
serviço do agente	sudo /etc/init.d/appassure-agent status
aavdisk	sudo /etc/init.d/appassure-vdisk status

Execução de scripts no Agent para Linux

O AppAssure fornece a capacidade de executar scripts Bourne Shell na máquina com o Agent para Linux antes e depois de uma transferência.

Scripts suportados no Agent para Linux

Os seguintes scripts são suportados no Agent para Linux. Ao utilizá-los, você deve adicioná-los ao local /opt/appassure/scripts.

NOTA: Observe que se um script não for executável, a tarefa de transferência falhará.

- PreTransferScript.sh
- PostTransferScript.sh

NOTA: Para obter mais informações sobre a forma de uso de scripts no AppAssure, bem como uma lista completa com todos os scripts suportados no Core, consulte o Apêndice A: Forma de uso de scripts no *Guia do usuário do Dell AppAssure*.

Parâmetros suportados para scripts de transferência e pós-transferência

Os seguintes parâmetros são suportados no Linux para scripts de transferência.

- TransferPrescriptParameter_VolumeNames=$TransferPrescriptParameter_VolumeNames
- TransferPrescriptParameter_ShadowCopyType=$TransferPrescriptParameter_ShadowCopyType
- TransferPrescriptParameter_TransferConfiguration=$TransferPrescriptParameter_TransferConfiguration
- TransferPrescriptParameter_StorageConfiguration=$TransferPrescriptParameter_StorageConfiguration

- TransferPrescriptParameter_Key=$TransferPrescriptParameter_Key
- TransferPrescriptParameter_ForceBaseImage=$TransferPrescriptParameter_ForceBaseImage
- TransferPrescriptParameter_IsLogTruncation=$TransferPrescriptParameter_IsLogTruncation
- TransferPrescriptParameter_LatestEpochSeenByCore=$TransferPrescriptParameter_LatestEpochSeenByCore

Os seguintes parâmetros são suportados no Linux para scripts de pós-transferência.

- TransferPostscriptParameter_VolumeNames=$TransferPostscriptParameter_VolumeNames
- TransferPostscriptParameter_ShadowCopyType=$TransferPostscriptParameter_ShadowCopyType
- TransferPostscriptParameter_TransferConfiguration=$TransferPostscriptParameter_TransferConfiguration
- TransferPostscriptParameter_StorageConfiguration=$TransferPostscriptParameter_StorageConfiguration
- TransferPostscriptParameter_Key=$TransferPostscriptParameter_Key
- TransferPostscriptParameter_ForceBaseImage=$TransferPostscriptParameter_ForceBaseImage
- TransferPostscriptParameter_IsLogTruncation=$TransferPostscriptParameter_IsLogTruncation
- TransferPostscriptParameter_LatestEpochSeenByCore=$TransferPostscriptParameter_LatestEpochSeenByCore

Instalação do AppAssure Central Management Console

O **AppAssure** Central Management Console fornece uma interface central para configurar e gerenciar vários cores.

> ⓘ **NOTA:** Você só precisa instalar o AppAssure Central Console caso seu ambiente contenha mais de um core.
>
> Além disso, observe que os sistemas operacionais Windows 8, 8.1 e Windows Server 2012, 2012 R2 precisam ter o recurso ASP.NET 4.5 instalado no servidor para que a GUI seja corretamente carregada. Esta configuração está incluída como parte do instalador do AppAssure.

Para instalar o AppAssure Central Management Console

1. Baixe o arquivo do instalador do AppAssure Central Console no website da **AppAssure**; por exemplo:

   `Central Console-X64-5.X.X.xxxxx.exe`

   > ⓘ **NOTA:** O AppAssure Central Management Console exige uma plataforma Windows de 64 bits. Sistemas de 32 bits não são suportados.

2. Clique em **Executar** ou **Salvar**.
   - Se você clicar em **Salvar**, selecione o local em que deseja salvar o arquivo.

     O arquivo será baixado em seu sistema. Navegue até o local em que você salvou o arquivo do instalador e dê um clique duplo nele. Você precisa executar o instalador com privilégios de administrador local.
   - Se você clicar em **Executar**, o instalador será iniciado automaticamente.

     > ⓘ **NOTA:** O instalador verifica se o .NET Framework 4.0 está instalado no seu sistema. Caso ausente, o instalador solicitará que você baixe e instale o Framework.

   O Assistente de instalação do AppAssure Central Console é exibido.

3. Na página Bem-Vindo, clique em **Avançar** para prosseguir com a instalação.

   A página Acordo de licença é exibida.

4 Clique em **Eu aceito os termos do acordo de licença** e, em seguida, clique em **Avançar**.

   A página Opções de instalação é exibida.

5 Confirme o caminho e a pasta de destino da instalação **e clique em Avançar**.

   - Caso queira especificar um caminho diferente, clique em **Alterar**, selecione o novo local e clique em **OK**.

   A página Progresso é exibida e inclui uma barra de status, que permite monitorar o progresso da instalação.

   Quando a instalação for concluída, a página Concluído será exibida.

6 Clique em **Concluir**.

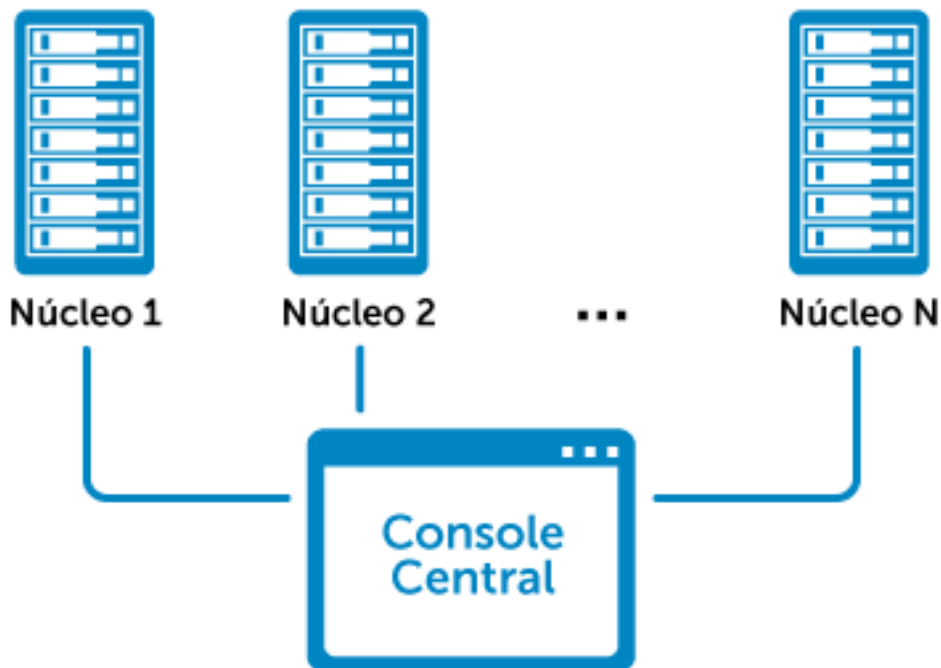
Configuração do AppAssure Central Management Console

Execute as etapas deste procedimento para instalar e configurar o AppAssure Central Management Console. Após concluir a configuração, será possível gerenciar as definições e todos os cores de um local central.

Para configurar o AppAssure Central Management Console

1 Faça login no AppAssure Central Management Console.

   A página Bem-Vindo é exibida. Na página Bem-Vindo, você pode identificar os grupos de Cores que você irá gerenciar no console.

   Figura 7. AppAssure Central Management Console - Guia Bem-Vindo

Adição de um grupo de Cores

Execute as etapas do procedimento a seguir para adicionar um grupo de Cores ao AppAssure Central Management Console.

Para adicionar um grupo de Cores

1 No AppAssure Central Management Console, clique em **Alternar para gerenciamento** e depois clique em **Adicionar grupo**.

A página Adicionar grupo é exibida.

2 Selecione o grupo principal e o nome de exibição conforme a descrição da tabela a seguir.

Tabela 8.

Caixa de texto	Descrição
Grupo principal	Selecione o grupo principal dos Cores para o novo grupo de Cores que você deseja adicionar.
Nome de exibição	Insira um nome para o grupo de Cores.

3 Clique em **Salvar**.

Configuração das definições do grupo de Cores

Execute as etapas do procedimento a seguir para configurar as definições do grupo de Cores.

Para configurar as definições de grupo de Cores

1 No AppAssure Central Management Console, clique em **Alternar para gerenciamento** e selecione o grupo de Cores.

A pagina Definições é exibida.

2 Na guia Definições, modifique as informações do grupo de Cores conforme as descrições da tabela a seguir.

Tabela 9.

Caixa de texto	Descrição
Grupo principal	Selecione o grupo principal dos Cores para as definições do novo grupo de Cores que você deseja adicionar.
Nome de exibição	Insira um nome para o grupo de Cores.

3 Clique em **Salvar**.

Configuração do acesso ao grupo de Cores

Execute as etapas do procedimento a seguir para configurar o acesso ao grupo de Cores.

Para configurar o acesso ao grupo de Cores

1 No AppAssure Central Management Console, clique em **Alternar para gerenciamento** e selecione o grupo de Cores.

A pagina Definições é exibida.

2 Clique na guia **Acesso**.

3 Clique em **Adicionar**.

A página Permitir acesso é exibida.

4 Na caixa de texto Nome, insira o nome do indivíduo para quem você deseja conceder os privilégios de acesso.

5 Clique em **Confirmar nome** para confirmar a validade do nome inserido.

Se o nome inserido for válido, uma mensagem indicando que a conta está confirmada será exibida.

> NOTA: É possível validar indivíduos e grupos.

6 Clique em **É um grupo** para especificar que o nome de um grupo foi anteriormente inserido na caixa de texto Nome.

7 Clique em **Salvar**.

As informações do grupo de Cores serão exibidas na guia Acesso.

Adição de um Core a um grupo de Cores

Execute as etapas do procedimento a seguir para adicionar um core a um grupo de Cores.

Para adicionar um Core a um grupo de Cores

1 No AppAssure Central Management Console, clique em **Alternar para gerenciamento** e depois clique em **Adicionar Core**.

A página Adicionar Core é exibida.

2 Insira as credenciais do grupo principal do Core conforme as descrições da tabela a seguir.

Tabela 10.

Caixa de texto	Descrição
Grupo principal	Selecione o grupo principal dos Cores para o novo Core que você deseja adicionar.
Nome de exibição	Insira um nome para o Core.
Nome do host	Insira um endereço IP para acessar o Core.
Porta	Insira um número de porta para a conexão. O valor padrão é *8006*.
Nome de usuário	Insira um nome de usuário para acessar o serviço de Core do Core recém-adicionado. NOTA: Esta é uma caixa de texto obrigatória.
Senha	Insira uma senha para acessar o serviço de Core para o Core recém-adicionado. NOTA: Esta é uma caixa de texto obrigatória.

3 Clique em **Testar conexão** para testar a configuração.

Se o teste for bem sucedido, uma mensagem será exibida para indicar que a conexão foi bem sucedida.

4 Clique em **Salvar**.

Configuração das definições do Core

Execute as etapas do procedimento a seguir para configurar as definições do Core.

Para configurar as definições do Core

1 No AppAssure Central Management Console, clique em **Alternar para gerenciamento** e selecione o grupo de Cores.

A pagina Definições é exibida.

2 Na guia Definições, modifique as informações do core conforme a descrição da tabela a seguir.

Tabela 11.

Caixa de texto	Descrição
Grupo principal	Selecione o grupo principal dos Cores para as novas definições do Core que você deseja adicionar.
Nome de exibição	Insira um nome de exibição para o Core.
Nome de usuário	Insira o nome de usuário do Core.
Senha	Insira a senha do Core.
Como o portal de gerenciamento deve se conectar ao [nome do core]?	Selecione a opção que especifica a conexão. Você pode selecionar: • Usar o último endereço IP (xxx.xxx.xxx.xxx) conhecido do [nome do core] ou • Usar o nome de host ou endereço IP. Se você optar por especificar a conexão através do uso de um nome de host ou endereço IP, é necessário inserir as informações apropriadas.
Em qual porta o [nome do core] está escutando?	Selecione uma das opções de porta. Você pode selecionar: • Porta padrão (8006) ou • Porta personalizada Se você optar por especificar uma porta, insira o número da porta na caixa de texto Porta personalizada.

3 Clique em **Testar conexão**.

Se o teste for bem sucedido, uma mensagem será exibida para indicar que a conexão foi bem sucedida.

4 Clique em **Salvar**.

Instalação automática de atualizações

Ao instalar o AppAssure Core, você pode optar por atualizar automaticamente o software AppAssure Core. Para saber as etapas específicas sobre como selecionar tais opções, consulte Instalação do AppAssure Core.

Também é possível optar por receber notificações quando uma versão atualizada do software do Core estiver disponível ou ignorar as atualizações. Após a conclusão da instalação, as definições podem ser alteradas a qualquer momento. Para obter mais informações sobre a alteração das definições de atualização automática, consulte o tópico Configuração das definições de atualização no *Guia do usuário do Dell AppAssure*.

Se você optar por atualizações automáticas, ou se optar por receber notificações sobre as atualizações, o software no AppAssure Core é verificado regularmente em relação às novas versões disponíveis no Portal de licenças do Dell AppAssure.

- Se você optar por atualizações automáticas, quando uma nova versão for detectada, a versão do Core será atualizada após a conclusão dos outros trabalhos noturnos agendados.
- Se você optar por receber notificações sobre as atualizações, quando uma nova versão for detectada, uma mensagem será exibida no Core Console abaixo da barra de botões indicando que uma nova versão está disponível e incluindo um link para obter a atualização.

A Dell recomenda usar a opção de atualização automática para ambientes que não utilizam replicação. A configuração padrão das atualizações automáticas é verificar semanalmente se há atualizações.

É possível alterar a frequência com que o sistema verifica as atualizações (as opções incluem diariamente, semanalmente, mensalmente ou nunca) a qualquer momento alterando as definições de atualização do Core na guia Configuração do AppAssure Core Console. Para obter mais informações sobre como alterar as definições, consulte o tópico Configuração das definições de atualização no *Guia do usuário do Dell AppAssure*.

Se estiver usando a replicação, a ordem recomendada para o upgrade dos componentes é sempre realizar primeiro o upgrade do core de destino, depois o upgrade do core de origem e, por fim, atualizar o software Agent nas máquinas protegidas.

△ CUIDADO: **O core de origem não deve executar uma versão do AppAssure mais recente do que a versão do core de destino. Para evitar conflito com o recurso de atualização automática, que pode atualizar máquinas na ordem errada, a Dell recomenda que, para ambientes de replicação, os administradores apliquem upgrades manualmente, em vez de usarem o recurso de atualização automática.**

Desinstalação do software do AppAssure Agent

Ao remover uma máquina da proteção no AppAssure Core, o software Agent não é afetado. Para remover o software AppAssure Agent de uma máquina, realize as etapas descritas nas seções seguintes conforme o sistema operacional da máquina.

Independentemente do sistema operacional, você deve reiniciar a máquina para concluir a remoção do software AppAssure Agent.

Esta seção inclui os seguintes tópicos:

- Desinstalação do software AppAssure Agent de uma máquina com Windows
- Desinstalação do software AppAssure Agent de uma máquina com Linux

Desinstalação do software AppAssure Agent de uma máquina com Windows

Execute as etapas descritas no procedimento a seguir para desinstalar o software AppAssure Agent de uma máquina com Windows.

Para desinstalar o software do Agent de uma máquina com Windows

1. No computador do qual você deseja desinstalar o software AppAssure Agent, abra o Painel de controle, clique em **Programas** e depois clique em **Desinstalar um programa**.
2. Na janela Programas e recursos, dê um clique duplo na versão instalada do software **AppAssure** Agent.

   O Assistente de instalação do AppAssure Agent é exibido, mostrando a página Reparar/Remover.
3. Clique em **Remover** e depois em **Avançar**.

   A página Remover opções é exibida.
4. Clique em Desinstalar as definições de configuração e dados, incluindo todas as imagens de cópia de segurança e logs de alteração? e depois clique em Desinstalar.

   A página Progresso é exibida. Você pode visualizar o progresso da ação de desinstalação na página Progresso.

   Quando a remoção for concluída, a página Concluído será exibida.
5. Na página Concluído, você vê uma mensagem indicando que o sistema deve ser reiniciado antes de a instalação entrar em vigor. Realize uma das seguintes ações e clique em Concluir:
   - Para reiniciar agora, selecione Sim, **desejo reiniciar meu computador agora.**
   - Para reiniciar mais tarde, desmarque a opção **Sim, desejo reiniciar meu computador agora.**

ⓘ NOTA: É preciso reiniciar o sistema para concluir a remoção do software do AppAssure Agent.

Desinstalação do software AppAssure Agent de uma máquina com Linux

Execute as etapas descritas no procedimento a seguir para desinstalar o software AppAssure Agent de uma máquina com Linux.

As instruções de desinstalação são diferentes dependendo da distribuição do Linux que você está usando. Para obter mais informações sobre a desinstalação do agente para Linux, consulte os seguintes tópicos:

- Desinstalação do software do Agent em sistemas Ubuntu
- Desinstalação do software do Agent em sistemas Red Hat Enterprise Linux e CentOS
- Desinstalação do software do Agent em sistemas SUSE Linux Enterprise Server

Desinstalação do software do Agent em sistemas Ubuntu

Execute as etapas abaixo para desinstalar o software AppAssure Agent em sistemas Ubuntu.

NOTA: As seguintes etapas se aplicam a ambientes de 32 e 64 bits.

Para desinstalar o software Agent em sistemas Ubuntu

1. Abra uma sessão do terminal com acesso raiz.
2. Altere para o diretório que inclui o script de instalação do AppAssure, por exemplo:

   `/home/appassure/.`
3. Insira o seguinte comando:

   ```
   ./appassure-installer_ubuntu_amd64_5.x.x.xxxxx.sh -u
   ```

   O sistema remove os arquivos e diretórios do AppAssure Agent.

Após a conclusão do processo, o software Agent será removido do sistema e a máquina não poderá mais ser protegida pelo Core.

Desinstalação do software do Agent em sistemas Red Hat Enterprise Linux e CentOS

Execute as etapas abaixo para desinstalar o software AppAssure Agent em sistemas Red Hat Enterprise e no CentOS.

NOTA: As seguintes etapas se aplicam a ambientes de 32 e 64 bits.

Para encontrar os números de compilação e versão específicos de seus arquivos do AppAssure Agent, execute o comando "`rpm -qa |grep appassure`" na sua sessão do terminal. Para sistemas RHEL e CentOS de 32 bits, a extensão de arquivo nas etapas abaixo será alterada de "x86_64" para "i386".

Para desinstalar o software Agent em sistemas Red Hat Enterprise Linux e CentOS

1. Abra uma sessão do terminal com acesso raiz.
2. Altere para o diretório que inclui o script de instalação do AppAssure, por exemplo: /home/appassure/.
3. Insira o seguinte comando:

   ```
   ./appassure-installer_rhel_amd64_5.x.x.xxxxx.sh -u
   ```

Após a conclusão do processo, o software Agent será removido do sistema e a máquina não estará mais protegida pelo Core.

Desinstalação do software do Agent em sistemas SUSE Linux Enterprise Server

Execute as etapas abaixo para desinstalar o software AppAssure Agent em sistemas SUSE Linux Enterprise Server (SLES).

ⓘ **NOTA:** As seguintes etapas se aplicam a ambientes de 32 e 64 bits.

Para desinstalar o software Agent em sistemas SUSE Linux Enterprise Server

1. Abra uma sessão do terminal com acesso raiz.
2. Altere para o diretório que inclui o script de instalação do AppAssure, por exemplo: /home/appassure/.
3. Insira o seguinte comando:

   ```
   ./appassure-installer_sles_amd64_5.x.x.xxxxx.sh -u
   ```

Após a conclusão do processo, o software Agent será removido do sistema e a máquina não estará mais protegida pelo Core.

Desinstalação do AppAssure Core

Execute as etapas deste procedimento para desinstalar o AppAssure Core.

Para desinstalar o AppAssure Core

1. No servidor Windows do qual deseja desinstalar o AppAssure Core, abra o Painel de controle, clique em **Programas** e depois clique em **Desinstalar um programa**.
2. Na janela Programas e recursos, dê um clique duplo na versão instalada da instância do **AppAssure** Core, por exemplo:

   ```
   Core-X64-5.x.x.xxxxx.exe
   ```

   O AppAssure Core Installation Wizard será exibido com a página Reparar/Remover.
3. Clique em **Remover** e depois em **Avançar**.

   A página Modificar definições será exibida.
4. Para remover o seu repositório, bem como todos os pontos de recuperação e logs de alterações, clique em **Desinstalar as definições de configuração e dados, incluindo todas as imagens de cópia de segurança e logs de alteração** e depois em **Avançar**.

   ⓘ **NOTA:** Se você selecionar esta opção, você excluirá **todos** os dados no repositório, incluindo a pasta do repositório e todas as suas subpastas. Esta opção é adequada para instalações em que o repositório é instalado em um volume vazio. Se você possuir outros dados no diretório em que se encontra o seu repositório, **não selecione essa opção**.

   A página Progresso é exibida. Você pode visualizar o progresso da desinstalação na página Progresso.

   Quando a desinstalação for concluída, a página Concluído será exibida.
5. Clique em **Concluir**.

Desinstalação do AppAssure Central Management Console

Execute as etapas deste procedimento para desinstalar o AppAssure Central Management Console.

Para desinstalar o AppAssure Central Management Console

1. No servidor Windows do qual deseja desinstalar o AppAssure Central Management Console, abra o Painel de controle, clique em **Programas** e depois clique em **Desinstalar um programa**.
2. Na janela Programas e recursos, dê um clique duplo na instância instalada do **AppAssure** Central Management Console, por exemplo:

   `Central Console-X64-5.x.x.xxxxx.exe`

   O Assistente de instalação do AppAssure Central Management Console será exibido com a página Reparar/Remover.
3. Clique em **Remover** e depois em **Avançar**.

   A página Modificar definições será exibida.
4. Clique em **Desinstalar as definições de configuração e dados, incluindo todas as imagens de cópia de segurança e logs de alteração** e depois em **Avançar**.

   A página Progresso é exibida. Você pode visualizar o progresso da desinstalação na página Progresso.

   Quando a desinstalação for concluída, a página Concluído será exibida.
5. Clique em **Concluir**.

3

Migrar do Replay 4 para o AppAssure

Este capítulo explica como migrar pontos de recuperação de um repositório do Replay 4 para um arquivo do AppAssure. É possível armazenar o arquivo para uso futuro com um Replay 4 Core, ou importar o arquivo para um AppAssure 5.3.x Core. (A Dell recomenda usar o AppAssure 5.3.7 Core.)

Depois de importar o arquivo para o AppAssure, os pontos de recuperação migrados serão representados no AppAssure Core como máquinas protegidas "apenas de pontos de recuperação". Isso pode ser usado para a recuperação no nível do arquivo, mas não para recuperação no nível de volume, exportação virtual ou bare metal restore.

NOTA: Para obter mais informações sobre máquinas apenas de pontos de recuperação, consulte o tópico "Visualizar a guia Início" no *Guia do usuário do AppAssure*.

Se você instalar o software AppAssure Agent nas mesmas máquinas representadas em máquinas apenas de pontos de recuperação, a primeira cópia de segurança salva é uma imagem de base integral. Esse processo estabelece uma nova cadeia de ponto de recuperação usando um ID de agente único. Portanto, é possível realizar toda a gama de operações do AppAssure com esses pontos de recuperação, incluindo restauração no nível do arquivo, restauração no nível do volume, exportação virtual e bare metal restore.

Se desejar usar o AppAssure versão 5.4 ou posterior, realize o upgrade do AppAssure 5.3.x Core para a versão 5.4. Para obter mais informações, consulte o tópico "Upgrade do AppAssure".

CUIDADO: Uma vez que versões do AppAssure posteriores ao AppAssure **5.3.7 representam pontos de recuperação em um formato diferente, os pontos de recuperação são convertidos após o upgrade. Este é um processo que ocorre apenas uma vez e não é compatível com versões anteriores.**

Planeje adequadamente. Na primeira vez que você iniciar o Core depois do upgrade do AppAssure versão 5.3.x para a versão 5.4.1 ou posterior, o carregamento dos pontos de recuperação existentes levará aproximadamente o dobro do tempo do carregamento dos mesmos pontos de recuperação nas versões anteriores. O tempo que leva para converter é diferente para cada ambiente do AppAssure, com base, em parte, na quantidade e no tamanho dos pontos de recuperação, da quantidade de memória no core e da taxa de transferência de rede disponível no momento da conversão. Depois da conversão inicial, o carregamento subsequente para pontos de recuperação no Core é significativamente menor que com versões anteriores.

Os seguintes tópicos estão incluídos:

- Noções básicas da Ferramenta de migração do AppAssure
- Migração dos pontos de recuperação
- Pré-requisitos para migrar o Replay 4 para AppAssure
- Migrar clusters
- Desinstalação do software do Replay 4 Agent
- Download e instalação da Ferramenta de migração do AppAssure
- Uso da Ferramenta de migração do AppAssure
- Importação de um arquivo

Noções básicas da Ferramenta de migração do AppAssure

Os pontos de recuperação criados usando o Replay 4 não são compatíveis com o AppAssure. Você deve usar a Ferramenta de migração do AppAssure para converter pontos de recuperação do Replay 4 para a estrutura do AppAssure 5.3.x criando um arquivo.

A Ferramenta de migração do AppAssure permite converter, arquivar e importar pontos de recuperação de um Replay 4 Core para um AppAssure Core. Depois de baixar e ativar o programa, o Assistente da ferramenta de migração do AppAssure irá guiá-lo pelas etapas de arquivamento e migração dos pontos de recuperação para o AppAssure Core.

△ CUIDADO: **Como a Ferramenta de migração do AppAssure não é diretamente compatível com a versão mais recente do AppAssure, recomenda-se primeiro migrar do Replay 4 para o AppAssure 5.3.7 e então imediatamente realizar o upgrade do Core para a versão mais recente do AppAssure antes de iniciar a implementação do software AppAssure Agent e a proteção de máquinas.**

Antes de começar, você precisará dos seguintes recursos:

- Replay 4 Core
- Dispositivo de armazenamento
- AppAssure Core

O dispositivo de armazenamento, como uma unidade USB, NAS, DAS ou SAN, é usado para armazenar temporariamente os pontos de recuperação arquivados até a importação para o AppAssure Core. Os pontos de recuperação do Replay 4 consistem em dados compactados, os quais são descompactados após a migração. Para compensar o pequeno aumento nos dados, a quantidade de espaço alocada no dispositivo deve ser pelo menos 30% maior do que a quantidade de espaço exibida para as máquinas que você deseja proteger.

O processo de migração de Replay 4 para AppAssure somente transfere os pontos de recuperação dos agentes selecionados. Ele não transfere definições de sistema configuradas em Agents e Cores do Replay 4. Para obter mais informações sobre as definições do AppAssure Core e Agent, consulte o *Guia do usuário do Dell AppAssure*.

Como os pontos de recuperação do Replay 4 não contêm todos os metadados encontrados nos pontos de recuperação do AppAssure, os pontos de recuperação migrados não terão funcionalidade total no AppAssure. Depois de importar o arquivo para o seu AppAssure Core, você poderá montar e explorar os pontos de recuperação migrados, bem como acessar dados como arquivos ou pastas, porém não poderá usá-los para realizar uma restauração no nível do volume, standby virtual ou bare metal restore.

A Dell recomenda que você se familiarize com os pré-requisitos para realizar a migração do Replay 4 para o AppAssure antes de começar para poder planejar seu tempo e seus esforços de acordo. Então execute os procedimentos conforme o documentado neste guia. Assumir essa abordagem resulta em mínimo tempo de inatividade e fornece o acesso mais rápido aos seus pontos de recuperação do Replay 4. Para informações sobre pré-requisitos, consulte o tópico "Pré-requisitos para migrar o Replay 4 para AppAssure".

Há duas abordagens básicas diferentes que você pode adotar para migrar do Replay para o AppAssure.

- Configure o novo ambiente do AppAssure em um servidor Windows dedicado usando o AppAssure 5.3.x. Use a Ferramenta de migração do AppAssure e importe o arquivo resultante para o novo Core. Retenha o servidor Replay Core existente no caso de ser necessário usá-lo no futuro.
- Use a Ferramenta de migração do AppAssure e transfira o arquivo resultante para um dispositivo de armazenamento. Limpe o servidor do Replay Core e configure-o como o seu novo AppAssure 5.3.x Core Server, garantindo que cumpra os requisito de tamanho adequados. Então importe o arquivo para visualizar e gerenciar os pontos de recuperação migrados no novo AppAssure Core.

Ambas as abordagens incluem as etapas descritas no tópico Processo de migração.

Migração dos pontos de recuperação

Em um alto nível, o processo de migrar pontos de recuperação envolve baixar a ferramenta, usar o assistente para criar um arquivo em um dispositivo de armazenamento e então importar o arquivo de um AppAssure Core. Na prática, muitas etapas são necessárias para preparar o Replay Core para arquivamento e para preparar um AppAssure 5.3.x Core para receber os pontos de recuperação, seguido pelo upgrade para a versão 5.4.3, se desejado.

Para migrar pontos de recuperação, execute as tarefas a seguir:

- **Etapa 1:** No Replay Core, desabilite as operações de rollup para todas as máquinas protegidas do Replay e interrompa todos os trabalhos. Para obter mais informações, consulte o tópico "Desativação do rollup para máquinas protegidas do Replay 4".
- **Etapa 2:** Copie as configurações de registro do Windows do servidor do Replay Core para um local de armazenamento. A cópia de segurança das configurações de registro não é feita usando a Ferramenta de migração do AppAssure. Para obter mais informações, consulte o tópico "Cópia e salvamento das definições de registro do Replay 4 Core".
- **Etapa 3:** Remova o software Replay Agent das suas máquinas protegidas. Para obter mais informações, consulte o tópico "Desinstalação do software do Replay 4 Agent".
- **Etapa 4:** No Replay Core, pare o serviço Replay Core. Para obter mais informações, consulte o tópico "Interrupção do serviço Replay 4 Core".
- **Etapa 5:** Obtenha e instale a Ferramenta de migração do AppAssure no seu Replay Core. Para obter mais informações, consulte o tópico "Download e instalação da Ferramenta de migração do AppAssure".
- **Etapa 6:** Execute o assistente da Ferramenta de migração do AppAssure para criar um arquivo dos seus dados do Replay. Salve o arquivo em um dispositivo de armazenamento ou unidade de rede adequados. Para obter mais informações, consulte o tópico "Uso da Ferramenta de migração do AppAssure".
- **Etapa 6:** Instale o AppAssure versão 5.3.x Core em um servidor Windows dedicado de tamanho adequado.

  NOTA: A Dell recomenda usar o AppAssure 5.3.7 Core. Para obter mais informações, consulte o *Guia de implementação doDell AppAssure* para a versão 5.3.7.

  Com base nos requisitos da sua empresa, esse é o mesmo servidor Windows físico (atualizado para as especificações atuais) ou um servidor Windows diferente.
- **Etapa 7:** Crie um repositório no AppAssure Core, no qual os pontos de recuperação migrados e os novos são armazenados. Para obter mais informações, consulte o tópico "Criar um repositório" no *Guia do usuário do Dell AppAssure*.
- **Etapa 8:** Importe o arquivo criado usando a Ferramenta de migração do AppAssure para o AppAssure 5.3.x Core. Para obter mais informações, consulte o tópico "Importação de um arquivo".
- **Etapa 9:** Determine se deseja instalar a versão mais recente do AppAssure.

  NOTA: A Dell recomenda instalar a versão mais recente do AppAssure. Consulte as *Notas de versão do AppAssure* para cada versão a fim de obter informações específicas, incluindo quaisquer orientações sobre versões recentes.
- **Etapa 10:** Realize o upgrade do software AppAssure Core, se adequado. Para obter mais informações, consulte o tópico "Upgrade do AppAssure".

  Se estiver usando a replicação, instale a mesma versão nos cores de origem e de destino, ou garanta que o core de destino contenha uma versão posterior. Para obter mais informações sobre a compatibilidade entre versões, consulte o tópico "Fatores de upgrade a considerar".
- **Etapa 11:** Instale o software AppAssure Agent (especificamente, a versão correspondente ao AppAssure Core) nas máquinas que deseja proteger. Para obter informações sobre a instalação do software Agent no AppAssure versão 5.3.7, consulte o *Guia de implementação do Dell AppAssure* para essa versão. Para obter informações sobre a instalação do software Agent em versões posteriores do AppAssure, consulte o tópico "Instalação do software do AppAssure Agent em máquinas com Windows" ou "Instalação do software do Agent em máquinas com Linux", respectivamente.

- **Etapa 12:** Comece a proteção dos AppAssure Agents usando o AppAssure Core. Você pode proteger uma única máquina usando o Assistente de proteção de máquina. Consulte o tópico Proteção de uma máquina no *Guia do usuário do Dell AppAssure*. Você também pode proteger diversas máquinas usando o Assistente de proteção de diversas máquinas. Consulte o tópico "Proteger várias máquinas" no *Guia do usuário do Dell AppAssure*.
- **Etapa 13:** Como opção, configure notificações para eventos. Consulte o tópico Configuração de grupos de notificação no *Guia do usuário do Dell AppAssure*. Se você deseja usar notificações por e-mail, isso inclui a configuração de um servidor SMTP (Simple Mail Transfer Protocol). Consulte o tópico "Configurar um servidor de e-mail" no *Guia do usuário do Dell AppAssure*.
- **Etapa 14:** Como opção, se você deseja usar chaves de criptografia para os dados do snapshot do agente, é necessário configurar chaves de criptografia para um ou mais agentes. É possível adicionar uma chave de criptografia ou importar uma chave de criptografia existente. Consulte os tópicos "Adicionar uma chave de criptografia" ou "Importar uma chave de criptografia", respectivamente, no *Guia do usuário do Dell AppAssure*.
- **Etapa 15:** Confirme se a instalação foi bem-sucedida e, de forma opcional (se instalado em uma nova máquina), desinstale o Replay 4 Core.
- **Etapa 16:** Revise a configuração do AppAssure regularmente para garantir que você tenha dedicado recursos suficientes.

  NOTA: A Dell recomenda revisar a configuração do AppAssure semestralmente. A melhor prática é revisar a quantidade de máquinas (e, possivelmente, os clusters de servidor) que você está protegendo: se você está usando a replicação, quanto tempo leva para os trabalhos noturnos serem concluídos e se a infraestrutura de rede é robusta o suficiente para suportar todas as operações do AppAssure, bem como as outras operações exigidas pela sua empresa.

  Para obter mais informações sobre dimensionamento de seu hardware, software, memória, armazenamento e requisitos de rede, consulte o artigo da Knowledgebase Dell AppAssure 118407, "Dimensionando implantações do AppAssure".

Pré-requisitos para migrar o Replay 4 para AppAssure

A instalação do AppAssure envolve instalar o AppAssure Core em uma máquina com Windows e os serviços do AppAssure Agent em máquinas com Windows e Linux. Se você planeja gerenciar vários Cores, instale também o AppAssure Central Management Console.

Para obter informações sobre os pré-requisitos do AppAssure Core, do AppAssure Agent e do AppAssure Central Management Console, consulte Requisitos para instalação.

Requisitos para instalação da ferramenta de migração AppAssure

Os requisitos de sistema para instalar a Ferramenta de migração do AppAssure estão descritos na tabela a seguir.

Tabela 12. Requisitos para instalação da ferramenta de migração AppAssure

Requisito	Detalhes
Sistema operacional	• Microsoft Windows XP SP3 (32 bits) • Microsoft Windows XP SP2 (64 bits) • Microsoft Windows Vista • Microsoft Windows 7 • Microsoft Windows Server 2003 • Microsoft Windows 2008 • Microsoft Windows 2008 R2
Arquitetura	somente 32 bits ou 64 bits
Memória	4 GB ou superior em um dispositivo de armazenamento temporário como uma unidade USB, NAS, DAS ou SAN.

Outros requisitos de instalação

Requisitos de chave ou arquivo de licença. Além dos requisitos de instalação descritos para os diversos componentes do AppAssure, também é necessário se registrar no Portal de licenças do Dell AppAssure, criar uma conta e obter uma chave ou arquivo de licença. A chave ou arquivo de licença são necessários para baixar o AppAssure Core e o software AppAssure Agent, assim como para configurar e proteger as máquinas.

Para obter mais informações sobre o Portal de licenças do Dell AppAssure, consulte o *Guia do usuário do portal de licenças do Dell AppAssure*, localizado no site de documentação do AppAssure em https://support.software.dell.com/appassure/release-notes-guides.

Requisitos de espaço de armazenamento. Analise a quantidade de espaço disponível no repositório antes de importar dados arquivados do Replay. Se a quantidade de espaço de armazenamento no repositório for limitada, considere reter o arquivo sem importar. Se precisar importar o arquivo no futuro, observe que deve importá-lo para um core do AppAssure 5.3.x e então realizar o upgrade desse core.

Migrar clusters

O AppAssure gerencia os clusters de maneira diferente do Replay 4. Enquanto o Replay 4 exibe os volumes compartilhados de um cluster como sendo parte de um agente ou outro (dependendo do horário do ponto de recuperação), o AppAssure e a Ferramenta de migração do AppAssure apresentam os volumes compartilhados de um cluster como máquinas protegidas separadas. Por exemplo, se o ambiente de um cluster contém duas máquinas, ele é exibido na Ferramenta de migração do AppAssure como três agentes: Nó A, Nó B e o cluster nomeado. Cada um dos nós contém os pontos de recuperação de seus volumes locais, enquanto o cluster nomeado contém os pontos de recuperação dos volumes do cluster compartilhado.

Depois de migrar os pontos de recuperação para o arquivo e importar o arquivo para o AppAssure Core, os nós e o cluster nomeado são exibidos como três agentes arquivados diferentes.

Para obter mais informações sobre o gerenciamento de clusters no AppAssure Core Console, consulte o *Guia do usuário do Dell AppAssure*.

Desinstalação do software do Replay 4 Agent

Execute as seguintes etapas para desinstalar os Agents do Replay 4:

- **Etapa 1**: Copie e salve as definições de registro do Replay 4 Core. Consulte Cópia e salvamento das definições de registro do Replay 4 Core.

- **Etapa 2:** Desative o rollup para todos os Agents do Replay 4. Consulte Desativação do rollup para máquinas protegidas do Replay 4.
- **Etapa 3**: Desinstale os Agents do Replay 4. Consulte Desinstalação do software do Replay 4 Agent.
- **Etapa 4**: Interrompa o serviço Replay 4 Core. Consulte Interrupção do serviço Replay 4 Core.

Cópia e salvamento das definições de registro do Replay 4 Core

Ao usar a Ferramenta de migração para converter pontos de recuperação visando efetuar a migração para o AppAssure, se certas ações (como rollups) ocorrerem durante a conversão, o processo poderá falhar. Por esse motivo, a Dell recomenda desativar o rollup e interromper o serviço Replay 4 Core antes de começar a migração. Antes de desativar o rollup, você precisa salvar as definições de registro do Replay 4 Core.

Para copiar e salvar as definições de registro do Replay 4 Core

1. Efetue login na máquina com o Replay 4 Core como usuário com privilégios de administrador.
2. Crie uma pasta para a qual você deseja copiar as definições do registro. Por exemplo, "C:\Backup".
3. Abra um Prompt de comando (cmd.exe) e digite:

   ```
   reg export hklm\software\appassure c:\Backup\appassure.reg
   ```

4. Substitua "C:\Backup\" pelo nome da pasta que você criou em Etapa 2.

   A pasta para onde você copiará as definições de registro precisa existir antes da execução do comando e você precisa ter direitos de acesso a ela.

5. Pressione **<Enter>**.

   ⓘ NOTA: Se as definições de registro do Replay 4 Core forem salvas no local especificado, você receberá a mensagem "A operação foi concluída com sucesso" no Prompt de comando.

   Se você receber a mensagem "ERRO: Não é possível gravar no arquivo. Pode haver um erro de sistema de arquivos ou disco", o caminho digitado não existe ou o programa reg.exe não pode criar o arquivo de definições de registro no caminho.

Desativação do rollup para máquinas protegidas do Replay 4

Depois de copiar e salvar as definições de registro do Replay 4 Core, você precisa desativar o rollup para as máquinas protegidas do Replay 4.

Para desativar o rollup para máquinas protegidas do Replay 4

1. No Replay Admin Console, clique com o botão direito em uma máquina protegida e selecione o menu Propriedades.

   A caixa de diálogo Propriedades é exibida.

2. Clique na guia Política de retenção.
3. Desmarque a caixa de seleção **Ativar rollup**.
4. Clique em **Salvar**.
5. Repita da Etapa 1 à Etapa 4 para cada máquina protegida do Replay 4 aplicável.

Desinstalação do software do Replay 4 Agent

Execute as etapas descritas neste tópico para desinstalar os Agents do Replay 4.

A desinstalação dos Agents do Replay 4 exige que a máquina seja reiniciada.

Para desinstalar o software Replay 4 Agent

1. No Painel de controle, clique em Programas e recursos.

   A tela Desinstalar ou alterar um programa é exibida.

2. Clique com o botão direito do mouse em Replay Agent e depois clique em **Alterar**.

   O Assistente do Install Shield do Replay Agent é exibido.

3. Clique em **Avançar**.

   A janela Manutenção do programa é exibida.

4. Selecione **Remover** e depois clique em **Avançar**.

   Uma tela de aviso é exibida.

5. Clique em **Remover** e depois em **Concluir**.

   O processo de desinstalação está concluído.

6. Reinicie a máquina.

7. Repita da Etapa 1 à Etapa 6 para cada Agent do Replay 4 aplicável.

Interrupção do serviço Replay 4 Core

Antes do processo de conversão, você precisa interromper o serviço Replay 4 Core. Isso evita que ocorra uma interferência na criação do arquivo do ponto de recuperação do Replay 4.

Para interromper o serviço Replay 4 Core

1. No menu Iniciar, clique em **Executar**.

   A janela Executar é exibida.

2. Na caixa de texto Abrir, digite:

   ```
   services.msc
   ```

3. Clique em **OK**.

   A janela Serviços é exibida.

4. Selecione **Serviço do Replay Core** na lista de serviços e clique em **Interromper o serviço**.

   O serviço Replay 4 Core agora está interrompido.

   > NOTA: Se você não interromper o serviço Replay 4 Core, a Ferramenta de migração do AppAssure solicitará que você interrompa o serviço antes de começar o processo de conversão. **Não reinicie o serviço do Replay 4 Core antes da conclusão do processo de conversão**. Para obter mais informações sobre a Ferramenta de migração do AppAssure, consulte Download e instalação da Ferramenta de migração do AppAssure.

Download e instalação da Ferramenta de migração do AppAssure

É possível baixar a Ferramenta de migração do AppAssure do Portal de licenças do Dell AppAssure. Execute as etapas do procedimento a seguir para baixar e instalar a Ferramenta de migração do AppAssure.

> **NOTA:** O instalador verifica se o .NET Framework 4.0 está instalado no seu sistema. Caso ausente, o instalador solicitará que você baixe e instale o Framework.

Para baixar e instalar a Ferramenta de migração do AppAssure

1. No Replay 4 Core, efetue login no Portal de licenças do Dell AppAssure em https://licenseportal.com.
2. No Portal de licenças, baixe a Ferramenta de migração do AppAssure de acordo com seu tipo de arquitetura. As seguintes opções estão disponíveis:
   - MigrationTool-x64-4.7.3.xxxxx para arquitetura de 32 bits
   - MigrationTool-x86-4.7.3.xxxxx para arquitetura de 64 bits

   Após a conclusão do download, clique duas vezes no ícone da Ferramenta de migração do AppAssure na sua área de trabalho para abrir o arquivo.

   Uma caixa de diálogo da ferramenta de extração instalada em sua máquina será exibida.
3. Na caixa de diálogo, clique em **Configurar** para extrair os arquivos compactados e prosseguir com a instalação.

   Uma barra de progresso monitora a extração dos arquivos e depois disso o Assistente do Install Shield para a Ferramenta de migração do AppAssure é aberto.
4. Na página Bem-Vindo do Assistente do Install Shield da Ferramenta de migração do AppAssure, clique em **Avançar**.

   A página Acordo de licença é exibida.
5. Na página Acordo de licença, selecione **Eu aceito os termos do acordo de licença** e, em seguida, clique em **Avançar**.

   A página Informações do cliente é exibida.
6. Na página Informações do cliente, insira o Nome de usuário e a Organização nas caixas de texto e depois clique em **Avançar**.

   A página Tipo de configuração é exibida.
7. Na página Tipo de configuração, selecione uma das opções descritas na tabela a seguir:

   Tabela 13.

Opção	Descrição
Completa	Todos os recursos do programa serão instalados. (Exige mais espaço em disco).
Personalizada	Escolha quais recursos do programa você deseja instalar e onde eles serão instalados. Recomendado para usuários avançados.

8. Clique em **Avançar**.

   A página Pronto para instalar o programa é exibida.
9. Na página Pronto para instalar o programa, clique em **Instalar** para começar a instalação. Uma barra de status permite monitorar o progresso da instalação.

   Quando a instalação for concluída, a página Assistente do Replay concluído será exibida.
10. Na página Assistente do Replay concluído, clique em **Concluir** para concluir a instalação e fechar o assistente.

    Um atalho para o arquivo executável da Ferramenta de migração do AppAssure será criado na sua área de trabalho.

Uso da Ferramenta de migração do AppAssure

Execute o procedimento a seguir para criar um arquivo dos pontos de recuperação usando o Assistente da Ferramenta de migração do AppAssure.

Recomenda-se efetuar a migração do arquivo com os pontos de recuperação para um dispositivo de armazenamento, como uma unidade USB, NAS, DAS ou SAN. A quantidade de espaço reservada no dispositivo deve ser pelo menos 30% maior do que a quantidade de espaço exibida para as máquinas que você deseja proteger, pois o volume dos dados do ponto de recuperação pode aumentar durante a migração.

Para usar o Assistente da Ferramenta de migração do AppAssure

1. No Replay 4 Core, clique duas vezes no ícone da Ferramenta de migração do AppAssure na sua área de trabalho.

   A ferramenta examina o repositório no Core. O tempo necessário para realizar o exame dependerá do número existente de agentes e pontos de recuperação.

   O Assistente da Ferramenta de migração do AppAssure é aberto na página Bem-Vindo.

2. Na página Bem-Vindo, clique em **Avançar** para continuar.

   A página Selecionar Agents é exibida.

3. Selecione as máquinas protegidas que deseja migrar e clique em **Avançar**.

   > **NOTA:** Você não precisa migrar todos os agentes de uma vez só; no entanto, todos os pontos de recuperação de cada agente precisam ser migrados. Além disso, você não pode selecionar e migrar pontos de recuperação específicos de um agente. Ao efetuar a migração de um agente, todos os pontos de recuperação para a máquina protegida são migrados no processo.

   - Caso você esteja realizando a migração de pontos de recuperação de um cluster, os nós do cluster e os volumes compartilhados são exibidos como agentes diferentes. Por exemplo, dois volumes compartilhados são exibidos como um único agente, com o nome do cluster relacionado na coluna Server protegido.
   - Se diversos agentes forem exibidos na lista, use a caixa de texto Filtrar para pesquisar agentes de acordo com um padrão ou com o nome do servidor.

     > **NOTA:** Ao procurar de acordo com um padrão, use um curinga (sinal "*") no lugar dos elementos desconhecidos do nome do servidor.

   - Se você estiver realizando a migração dos agentes em sessões separadas por razões de consumo de espaço em disco, marque a caixa de seleção **Ocultar agentes migrados** para exibir somente as máquinas protegidas que ainda não foram migradas.

     > **NOTA:** Ao selecionar as máquinas protegidas que serão migradas, reserve pelo menos 30% a mais de espaço no dispositivo de armazenamento do que o exibido na ferramenta para levar em conta a expansão que ocorre durante a migração. Use a barra de rolagem horizontal para visualizar a coluna Tamanho e verificar a quantidade de espaço em disco usada por cada agente.

   A página Definições de arquivo é exibida.

4. Na página Definições de arquivo, execute as seguintes etapas:

   a. Insira ou selecione o caminho para o local de arquivo clicando em **Procurar**.

   b. Se o local de arquivo estiver localizado em uma rede (recomendado), insira o Nome de usuário e a Senha do servidor.

   c. Selecione o tamanho máximo para o arquivo. Você pode selecionar **Destino inteiro** ou usar o seletor localizado próximo da caixa de texto para dividir o arquivo em volumes com tamanhos específicos.

d Clique em **Avançar**.

> NOTA: Conforme a Ferramenta de migração do AppAssure efetua a migração dos pontos de recuperação compactados, o volume dos dados aumenta. Leve em consideração os requisitos de espaço em disco para as máquinas protegidas sendo migradas para garantir que o volume de dados aumentado seja manuseado corretamente.

A página Conversão é exibida.

5 Clique em **Avançar** para começar a converter os dados para as máquinas protegidas.

Se o serviço Replay Core estiver em execução, uma mensagem avisará que a migração não deve ser realizada até que o serviço seja interrompido. Para prosseguir, escolha uma das seguintes opções:

- Clique em **Não** para continuar sem interromper o serviço Replay 4 Core.

> NOTA: O serviço Replay 4 Core poderá interferir no processo de conversão. O estado do serviço não será confirmado durante e conversão.

- Clique em **Sim** para salvar o estado do serviço Replay 4 Core e então interromper e desativar o serviço.

> NOTA: Para evitar interferências na criação do arquivo, não reinicie o serviço Replay 4 Core enquanto a conversão estiver em progresso. A Ferramenta de migração do AppAssure confirmará periodicamente se o serviço foi desativado e tentará desativá-lo novamente, caso ele seja reiniciado. Se a ferramenta não for capaz de desativar o serviço, uma mensagem será exibida lhe oferecendo a opção de desativar o serviço ou continuar a conversão com o serviço em execução.

A página Conversão em progresso será exibida, mostrando uma barra de progresso com informações sobre o status da conversão.

> NOTA: Se a quantidade de espaço no caminho de saída designado for muito pequena, ou caso você tenha decidido dividir o arquivo em vários arquivos menores, a página Próximo segmento de arquivo será exibida para que você selecione um caminho de saída adicional.

> CUIDADO: **Ao salvar os dados em múltiplos segmentos de arquivo, atribua um número a cada segmento. Os segmentos precisam ser importados para o AppAssure Core na ordem correta para que a migração ocorra com sucesso.**

A página Conversão concluída é exibida.

6 Clique em **Concluir**.

Se você decidir interromper o serviço Replay 4 Core, a Ferramenta de migração do AppAssure restaurará o serviço para o estado no qual ele foi salvo.

Importação de um arquivo

Quando desejar recuperar dados arquivados, é preciso importar o arquivo inteiro a um local especificado. Depois, você poderá procurar os dados. Para importar um arquivo, execute as etapas do procedimento a seguir.

Para importar um arquivo

1 Navegue até o AppAssure Core Console e selecione a guia Ferramentas.

2 Na opção Arquivo, clique em **Importar**.

3 Para **Tipo de localização**, selecione uma das seguintes opções na lista suspensa:

- Local
- Rede
- Nuvem

4 Insira os detalhes do arquivo, como descrito na tabela a seguir, com base no tipo de localização que você selecionou na Etapa 3.

Tabela 14.

Opção	Caixa de texto	Descrição
Local	Local	Insira o caminho para o arquivo.
Rede	Local	Insira o caminho para o arquivo.
	Nome de usuário	Insira o nome de usuário. Ela é usada para estabelecer credenciais de login para o compartilhamento de rede.
	Senha	Insira a senha para o caminho da rede. Ela é usada para estabelecer credenciais de login para o compartilhamento de rede.
Nuvem	Conta	Selecione uma conta da lista suspensa. NOTA: Para selecionar uma conta da nuvem, você deve primeiro tê-la adicionado no Core Console.
	Contêiner	Selecione um contêiner associado à sua conta no menu suspenso.
	Nome da pasta	Insira o nome da pasta na qual os dados arquivados são salvos, por exemplo, AppAssure-5-Arquivo-[DATA DE CRIAÇÃO]-[HORA DE CRIAÇÃO]

5 Clique em **Verificar arquivo** para validar a existência do arquivo a ser importado.

6 Na caixa de diálogo, verifique o nome do core de origem exibido na lista suspensa do Core.

7 Selecione os agentes a serem importados do arquivo.

8 Selecione o repositório no qual os dados arquivados serão salvos.

> NOTA: O repositório selecionado deve ser o mesmo repositório em que todos os atuais pontos de recuperação para o agente selecionado são armazenados.

9 Clique em **Restaurar** para importar o arquivo.

4

Upgrade do AppAssure

Este capítulo descreve como realizar o upgrade de uma instalação do AppAssure 5.3.x para a versão mais recente do AppAssure 5.4.x, ou como realizar o upgrade de uma versão anterior do AppAssure 5.4.x (beta, 5.4.1 ou 5.4.2) para a versão atual (5.4.3). Os seguintes tópicos estão incluídos:

- Fatores de upgrade a considerar
- Etapas de upgrade
- Aplicação de uma nova chave ou arquivo de licença

Realizar o upgrade para a versão mais recente do AppAssure 5.4.x garante que seu ambiente esteja equipado com as últimas correções e aprimoramentos disponíveis. Porém, realize o upgrade apenas depois de considerar cuidadosamente o efeito que isso pode ter sobre suas máquinas. Leia este capítulo por completo antes de decidir se deseja realizar o upgrade para AppAssure 5.4.x.

NOTA: Para obter informações sobre a migração de um ambiente do Replay 4 para o AppAssure, consulte Migrar do Replay 4 para o AppAssure.

Fatores de upgrade a considerar

Ao atualizar a versão do AppAssure em suas máquinas, é importante ter em mente as seguintes práticas recomendadas:

- Sempre realize o upgrade do Core antes do upgrade das máquinas protegidas com o software do AppAssure Agent.
- A máquina do core pode executar uma versão do AppAssure que é a mesma, ou mais recente, que a versão instalada nas máquinas protegidas.
- As máquinas protegidas não devem executar uma versão do AppAssure mais recente do que a versão instalada no core. Essa diretriz se aplica aos primeiros três dígitos no nome de uma versão (por exemplo, 5.3.7 ou 5.4.2).

NOTA: Dentro de uma versão, é aceitável usar diferentes números de compilação. Por exemplo, se usar a implementação em massa ou atualização automática, podem existir pequenas diferenças entre as versões de software do Agent ou entre a versão Agent e Core.

- A ordem recomendada dos componentes de atualização seria primeiro o core e depois as máquinas protegidas.
- Se usar a replicação, sempre atualize o core de destino primeiro, depois o core de origem e, por fim, as máquinas protegidas.

  CUIDADO: Para evitar conflito com o recurso de atualização automática do AppAssure, que pode realizar o upgrade de máquinas na ordem incorreta, a Dell recomenda que, para usuários de replicação, os administradores apliquem os upgrades manualmente (primeiro para os cores de destino, então para cores de origem e, por fim, para máquinas protegidas).

- O core de origem não deve executar uma versão do AppAssure mais recente do que a versão do core de destino.
- Se estiver usando replicação de cores (quando dois Cores são agentes de replicação um do outro), ambos os Cores devem passar por upgrade antes de reiniciarem as funções de replicação.

Upgrade do 5.2.x para o 5.4.x

Esteja ciente das seguintes informações ao realizar o upgrade do AppAssure 5.2.x para o AppAssure versão 5.4.1 e posteriores.

- O AppAssure está localizado em vários idiomas a partir da versão 5.4.2 internacional e posteriores. Se uma versão localizada do AppAssure for instalada, você poderá ver ou alterar o idioma de exibição atual definido para o AppAssure Core nas definições gerais de configuração do Core. Se estiver realizando o upgrade do AppAssure 5.2.2 para uma versão localizada do AppAssure, e não puder ver o parâmetro de idioma atual nas definições gerais de configuração do Core, consulte o Artigo 134116 da knowledgebase do Dell AppAssure.

Upgrade do 5.3.x para o 5.4.x

Esteja ciente das seguintes informações ao realizar o upgrade do AppAssure 5.3.x para o AppAssure versão 5.4.1 e posteriores.

- Se estiver usando o AppAssure Core versão 5.3.x, antes de realizar o upgrade, verifique se você tem binários personalizados aplicados. Fazer isso pode aumentar a capacidade do Suporte do Dell AppAssure de ajudá-lo no caso de dificuldades com o upgrade. Para obter mais informações, consulte o artigo 132353 da knowledgebase.
- Como parte das alterações feitas para melhorar o desempenho do aplicativo no AppAssure versão 5.4.x, os pontos de recuperação são representados de maneira diferente que em versões anteriores. Ao realizar o upgrade do AppAssure 5.3.x para o AppAssure 5.4.1 e posteriores, os pontos de recuperação existentes são convertidos para a nova representação, que não é compatível com versões anteriores. Não é possível fazer o downgrade de uma instalação do 5.4.x para 5.3, a menos que você recrie seu repositório.
- Ao iniciar o core pela primeira vez após realizar o upgrade de versões anteriores para o AppAssure AppAssure 5.4.1, a conversão de pontos de recuperação existentes levará aproximadamente o dobro do tempo do carregamento dos mesmos pontos de recuperação nas versões anteriores. No entanto, após essa conversão inicial, carregar pontos de recuperação será significativamente mais rápido do que nas versões anteriores.

  > **NOTA:** Ao realizar o upgrade do AppAssure 5.3.x para o 5.4.x, considere um tempo extra para converter os pontos de recuperação no seu planejamento antes de o ambiente do upgrade estar pronto para uso.

- Depois de realizar o upgrade de versões anteriores para o AppAssure 5.4.1, se você tentar configurar uma política de retenção em um core de destino replicado que seja diferente da política de replicação no core de origem, será solicitado a realizar um trabalho de verificação de integridade do repositório. O mesmo requisito se aplica se você desejar configurar uma política de retenção personalizada para um agente replicado. Executar esse trabalho pode identificar antecipadamente inconsistências nos pontos de recuperação replicados, oferecendo a oportunidade de substituir aqueles com pontos de recuperação livres de erro.

  > **CUIDADO: A execução do trabalho de verificação de integridade deve levar um longo tempo. O tempo necessário difere para cada ambiente conforme a quantidade e o tipo de dados no repositório e também conforme o sistema de armazenamento subjacente. Enquanto o trabalho está em execução, nenhuma outra transação pode ser executada naquele repositório, incluindo transferências (cópias de segurança do Snapshot e da imagem de base, e replicação), trabalhos noturnos e assim por diante. Não deixe de considerar o tempo extra para concluir um trabalho de verificação de integridade demorado no seu planejamento se essas situações se aplicarem a você.**

- Se você decidir não instalar essa versão e estiver usando um AppAssure versão 5.3.6 ou mais antigo, a Dell Software recomenda a atualização para o AppAssure 5.3.7 para que você aproveite as últimas correções. Para obter mais informações sobre o AppAssure 5.3.7, consulte as Notas de versão do AppAssure 5.3.7.

Upgrade do 5.4.x

Esteja ciente das seguintes informações ao realizar o upgrade de uma versão anterior do AppAssure versão 5.4.x para a versão atual.

- Usuários de qualquer versão beta 5.4 devem atualizar todos os cores e agentes para a versão 5.4.1.77 ou posterior, e é recomendável que atualizem para a versão 5.4.2. A interoperabilidade de versões beta e versões de produção não é suportada.
- Se estiver usando o AppAssure Core versão 5.4.1 ou superior, antes de realizar o upgrade, verifique se você tem algum binário personalizado aplicado. Na máquina core, abra Programas e Recursos no painel de controle e procure um programa rotulado no formato P-###### (por exemplo, P-000966). Se qualquer programa desse tipo estiver listado, anote-o para seus registros. Isso aumentará a capacidade do Suporte do Dell AppAssure de auxiliá-lo caso você encontre dificuldades durante o upgrade.

Etapas de upgrade

Ao atualizar o AppAssure, realize as seguintes etapas:

1. Revise os fatores de upgrade, como compatibilidade, cenários de replicação e práticas recomendadas.
2. Confirme que os Cores podem contatar o servidor de licença:
   a. Navegue até o AppAssure Core Console e clique na guia Configuração.
   b. Clique em **Aplicação de licença**.
   c. Na opção Server de licenças, clique em **Entrar em contato agora**.
3. Nas máquinas de Core das quais deseja realizar o upgrade, navegue para o portal de licenças em https://appassure.licenseportal.com e baixe o programa Core Installer, mas não o ative ainda.
   a. No portal de licenças, no lado esquerdo da página, clique em **Downloads**.
   b. Localize o Core Installer adequado no lado direito da página e clique em **Baixar**.
   c. Não ative o instalador ainda.
4. Baixe a versão correspondente do software do AppAssure Agent em cada máquina que deseje proteger.
   - Para cada máquina protegida, é possível seguir o mesmo processo descrito em Etapa 3, acessando o portal de licenças da máquina que deseja proteger e baixando manualmente o instalador do software do Agent adequado ao sistema operacional.
   - Como alternativa, você pode implementar o software em várias máquinas ao mesmo tempo usando o processo de implementação em massa do AppAssure Core. Para obter mais informações, consulte o tópico "Implementar em várias máquinas" no *Guia do usuário do Dell AppAssure*.

   d. Não ative o instalador ainda.
5. Para cada Core que desejar realizar o upgrade, pause e desative todas as atividades de transferência de dados, incluindo replicação, snapshots e trabalhos noturnos. Fazer isso acelera o processo de desligamento do serviço do AppAssure Core durante o upgrade. Para obter informações sobre como pausar atividades, consulte o *Guia do usuário do Dell AppAssure*.
6. Execute os programas do instalador em cores e máquinas protegidas, seguindo a ordem de upgrade descrita em Etapas de upgrade.
7. Reinicie todas as máquinas em que você instalou o software do AppAssure Agent.
8. Aplique novas chaves de licença nos Cores adequados, como descrito em Aplicação de uma nova chave ou arquivo de licença.
9. Retome a proteção em todos os Cores, então reinicie a replicação e os trabalhos noturnos.

Monitore as transferências iniciais pra garantir que o upgrade esteja livre de erros.

Aplicação de uma nova chave ou arquivo de licença

Durante a primeira inscrição para testar o AppAssure, você recebe uma conta de teste. A chave de licença de teste é automaticamente gerada quando você baixa o software AppAssure Core do Portal de licenças de software da Dell. Essa chave de licença é gravada no instalador do software AppAssure Core para que você instale o software. Para solicitar uma atualização de sua licença, entre em contato com o representante de vendas da Dell Software ou envie um e-mail para upgrade@apppassure.com. Depois de ter realizado o upgrade ou comprado a licença do AppAssure, é enviado um e-mail incluindo a nova chave ou arquivo de licença. Realize o seguinte procedimento para inserir essa chave ou arquivo de licença no Core Console.

Para aplicar uma nova chave ou arquivo de licença

1. Registre-se para uma conta no Portal de licenças de software da Dell em http://license.appassure.com. Registre-se usando o endereço de e-mail que está no arquivo com seu representante de vendas da Dell Software.
2. Após o registro de conta bem-sucedido, faça logon no Portal de licenças e depois clique em **Downloads** na área de navegação esquerda.
3. Para baixar e instalar o software Core, na página Downloads, clique no botão **Baixar** ao lado do Core Installer ou Core Web Installer, conforme apropriado.

> **NOTA:** O Core Installer baixa o arquivo executável em uma tarefa, enquanto o Core Web Installer transmite um download da versão mais recente do AppAssure Core installer, que é executada diretamente da Web e permite pausar e retomar o processo conforme o necessário. Uma chave de licença de teste é automaticamente gerada e apresentada para você para usá-la para o Core. A chave de licença também é exibida no e-mail de confirmação que você recebe depois de escolher a opção de download.

4. Clique em **Executar** nas caixas de diálogo subsequentes para instalar o software.
5. Para baixar e instalar o software do Agent, na página Downloads, ao lado da versão do Agent Installer de Windows ou Linux que deseja baixar, clique em **Baixar**.
6. Clique em **Executar** nas caixas de diálogo subsequentes para instalar o software.
7. Depois de instalar o software, abra o AppAssure Core Console para realizar o upgrade da licença de avaliação para a licença comprada ou de upgrade.
8. Navegue até a guia **Configuração** e clique em **Aplicação de licença**.
9. No painel Detalhes da licença, clique em **Alterar licença.**
10. Na caixa de diálogo Alterar licença, para carregar um arquivo de licença, faça o seguinte:
    - Selecione **Atualizar arquivo de licenças** e clique em **Procurar**.
    - Na caixa de diálogo Carregamento de arquivo, localize e selecione o arquivo de licença e clique em **Abrir**.
11. Ou, na caixa de diálogo Alterar licença, para inserir uma chave de licença, faça o seguinte:
    - Selecione **Inserir chave de licença**.
    - No campo de texto chave de licença, insira a chave de licença e clique em **Continuar**.
12. Em Servidor de licenças, clique em **Entrar em contato agora**. Assim que a licença for aplicada ao servidor de licenças, todos os agentes associados serão atualizados automaticamente com a nova licença.

Sobre a Dell

A Dell escuta os clientes e fornece tecnologia inovadora, soluções empresariais e serviços globais de confiança e valor. Para obter mais informações, visite www.software.dell.com.

Contatos da Dell

Suporte técnico:
Suporte online

Vendas e dúvidas sobre produtos:
(800) 306-9329

E-mail:
info@software.dell.com

Recursos do suporte técnico

O suporte técnico está disponível para clientes que compraram produtos de software da Dell com um contrato de manutenção válido e clientes que estão usando versões de teste. Para acessar o Portal de suporte, visite http://software.dell.com/support/.

O Portal de suporte fornece ferramentas de autoajuda, que você pode usar para resolver problemas de forma rápida e independente, 24 horas por dia, 365 dias por ano. Além disso, o Portal fornece acesso direto a engenheiros de suporte de produtos por meio de um sistema online de Solicitação de serviço.

O site permite que você:

- Crie, atualize e gerencie as Solicitações (casos) de serviço.
- Visualize artigos da Base de conhecimento.
- Obtenha notificações de produtos.
- Baixe o software. No caso de software de teste, acesse Downloads de teste.
- Assista a vídeos instrucionais.
- Participe de discussões da comunidade.
- Converse com um engenheiro do suporte.